CYBER FORENSICS

A PRACTICAL REPORT

ON

CYBER FORENSICS

SUBMITTED BY

Mr. BHAVISHAY MANKANI

Roll No: 22009

UNDER THE GUIDANCE OF

PROF. ANSHIKA GAUTAM

Submitted in fulfilment of the requirements for qualifying

MSc. IT Part II Semester - IV Examination 2023-2024

University of Mumbai

Department of Information Technology

R.D. & S.H National College of Arts, Commerce & S.W.A. Science College Bandra (West), Mumbai – 400 050

R. D. & S. H. National & S. W. A. Science College

Bandra (W), Mumbai - 40050

Department of Information Technology
M.Sc. (IT – SEMESTER IV)

Certificate

*This is to certify that **Cyber Forensics Practical's** performed at R.D & S.H National & S.W.A. Science College by Mr. **Bhavishay Mankani** holding Seat No. _____ studying Master of Science in Information Technology Semester – IV has been satisfactorily completed as prescribed by the University of Mumbai, during the year 2023 – 2024*

Subject In-Charge **Coordinator In-Charge** **External Examiner**

College Stamp

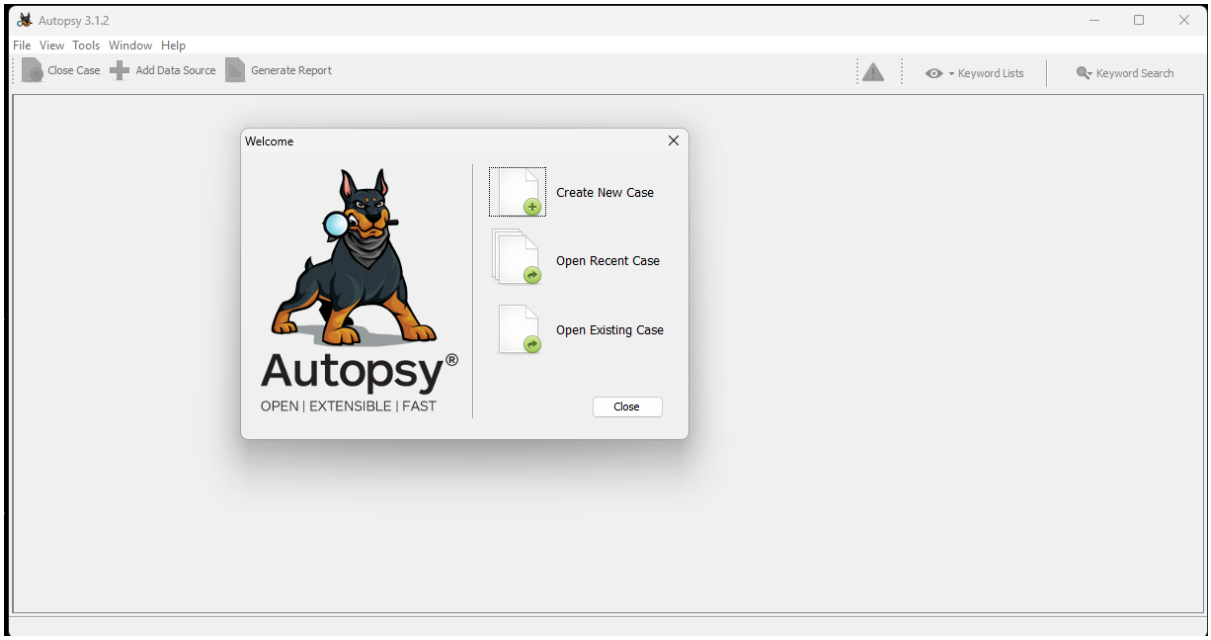
INDEX

Practical: 1

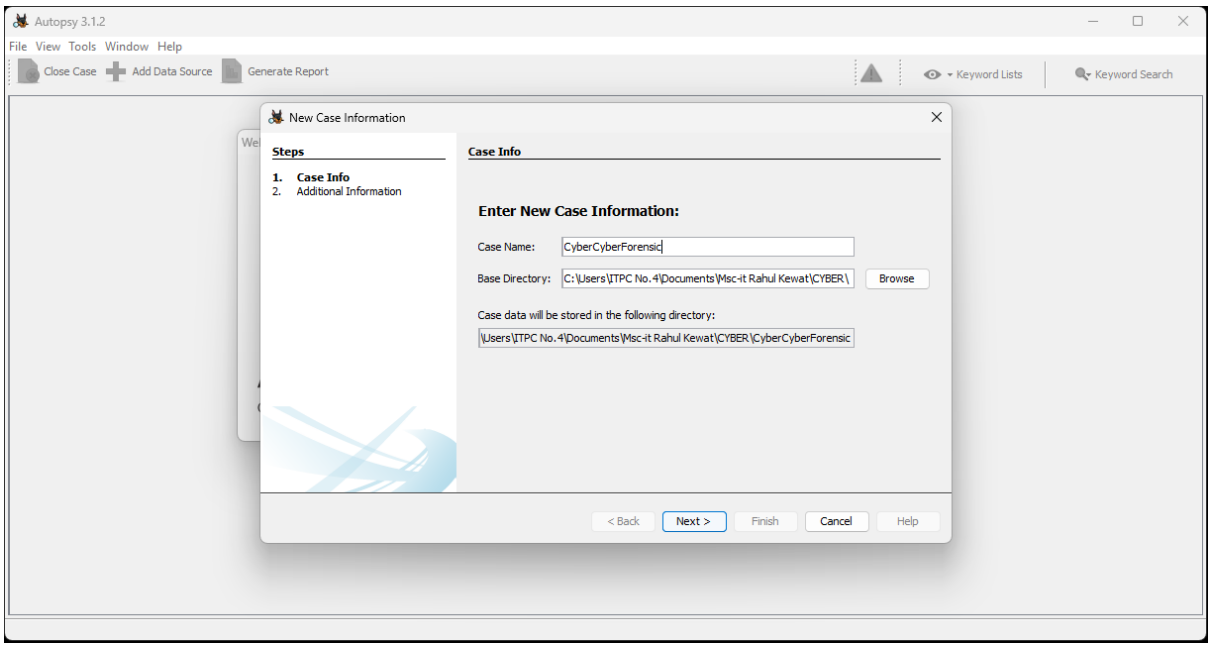
Aim: File system Analysis using The Sleuth kit.

Writeup:

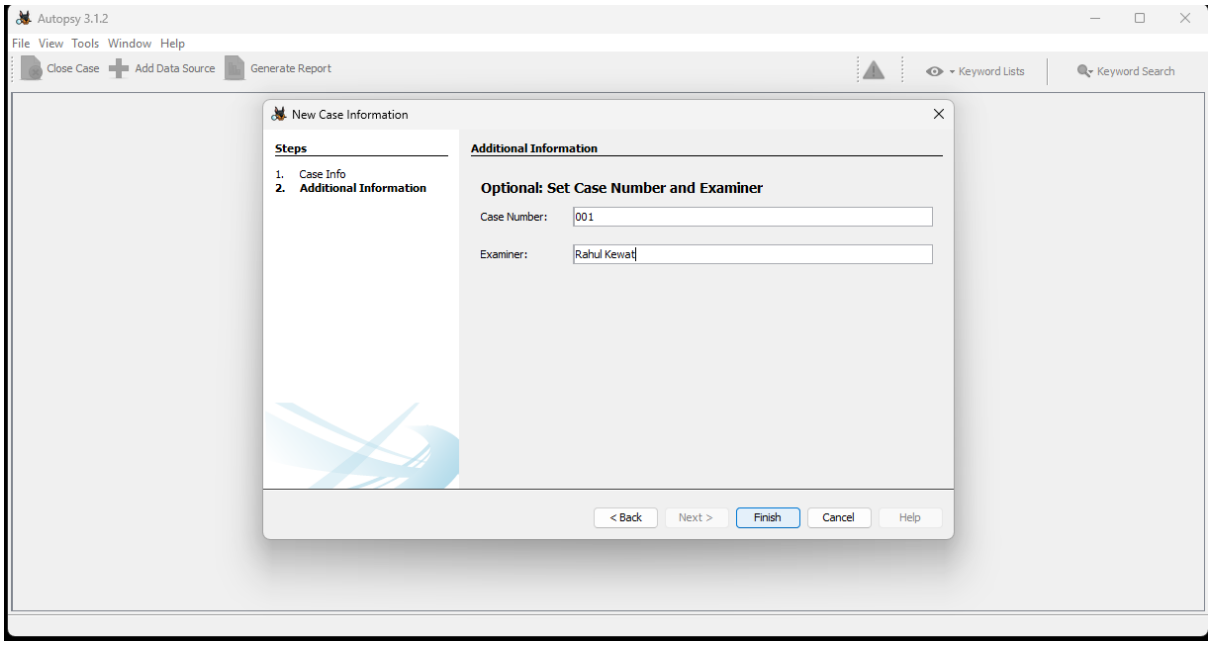
Step 1: Open **Autopsy 3.12** and Click on **Create New Case**



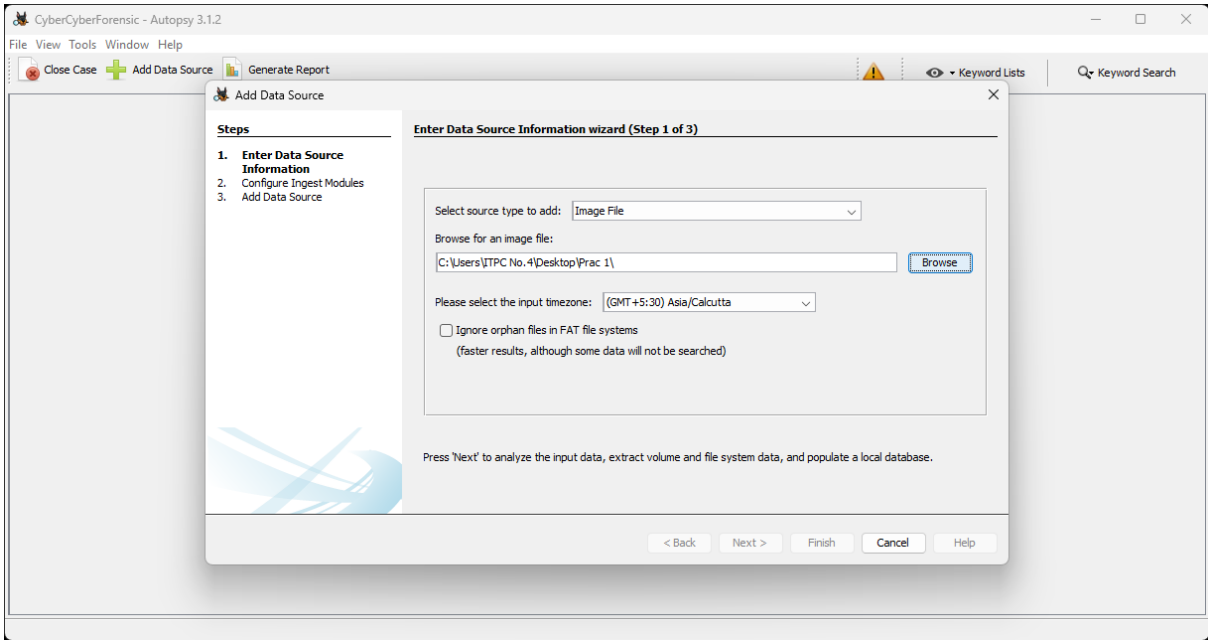
Step 2: Within **Enter New Case Information** Type Case Name **(Here it is CyberForensic)** and **Click on Browse** and Select **Base Directory** and **Click on Next**



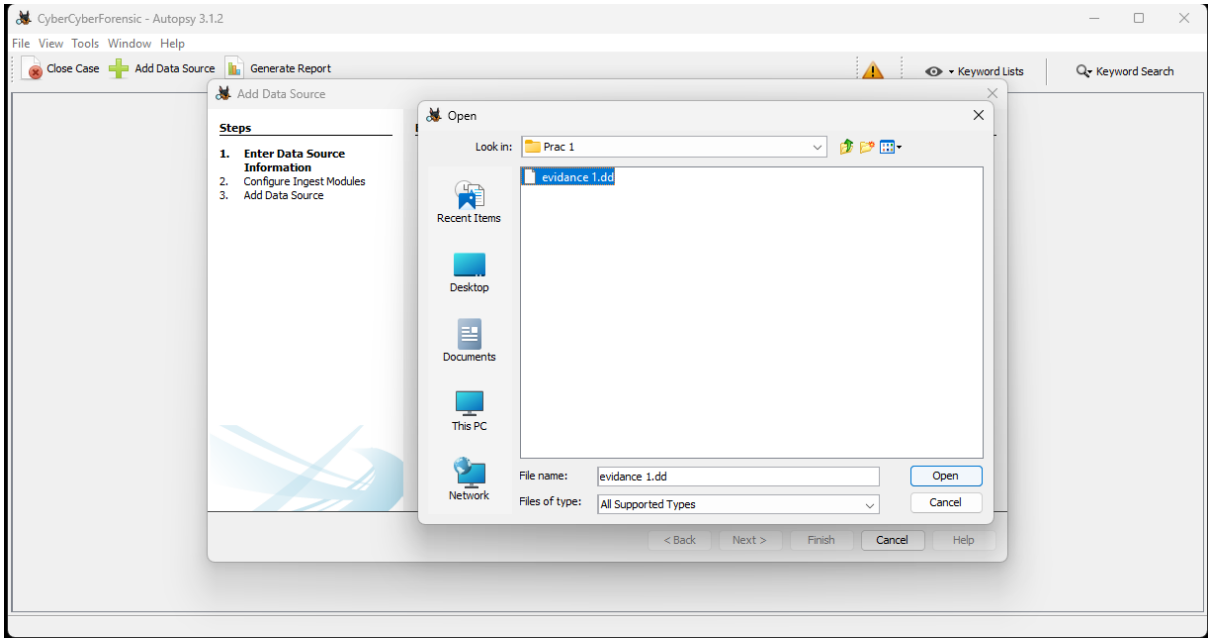
Step 3: Within **Additional Information Set Case Number and Examiner** Here it is **Case Number 001** And **Examiner Name Rahul Kewat** and **Click on Finish**



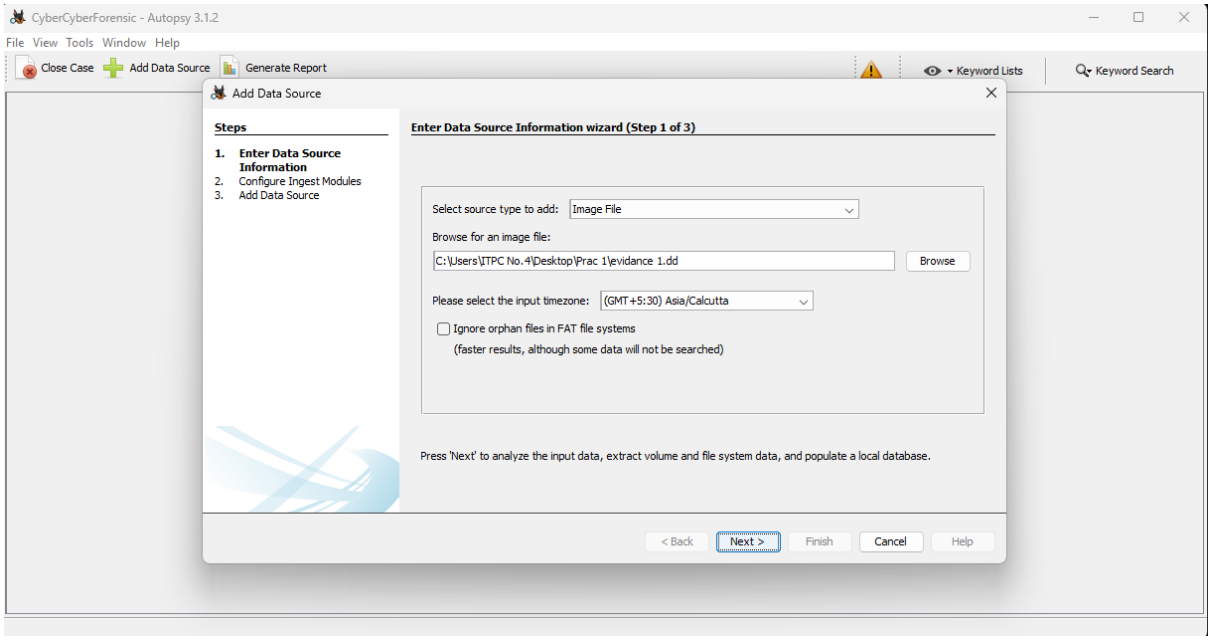
Step 4: The next step in the investigation will be to add an image file to the case. Within **Enter Data Source Information Select source type to add: Here we select Image File** and **Click on Browse**



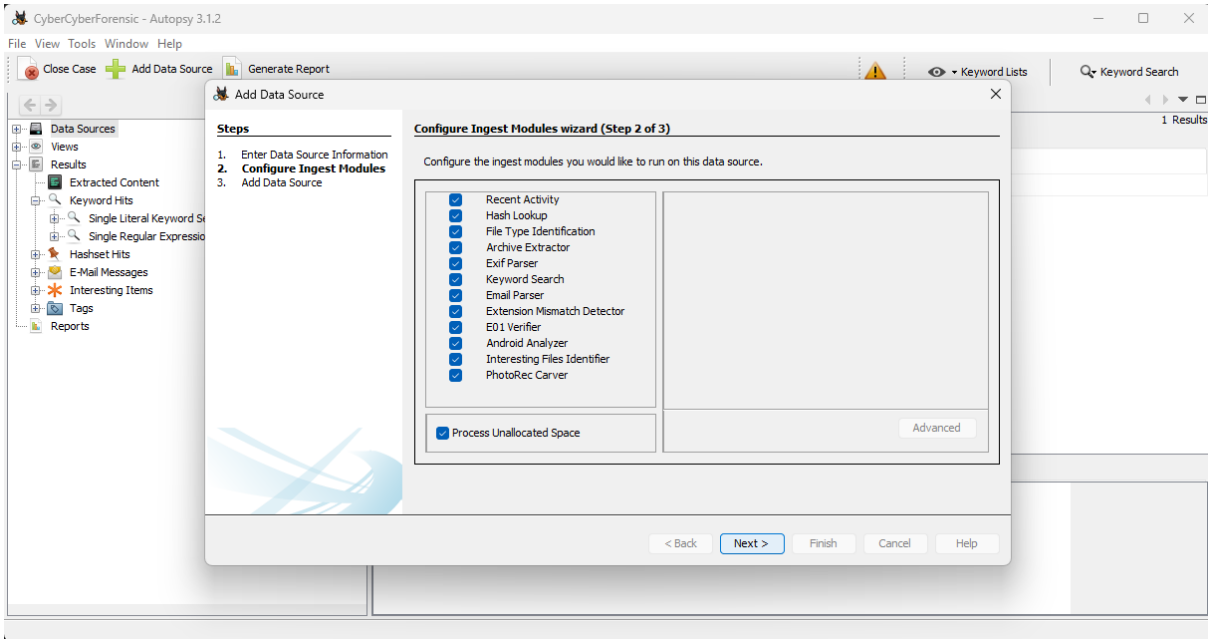
- After **Click on Browse** Select **evidance1.dd Click on Open**



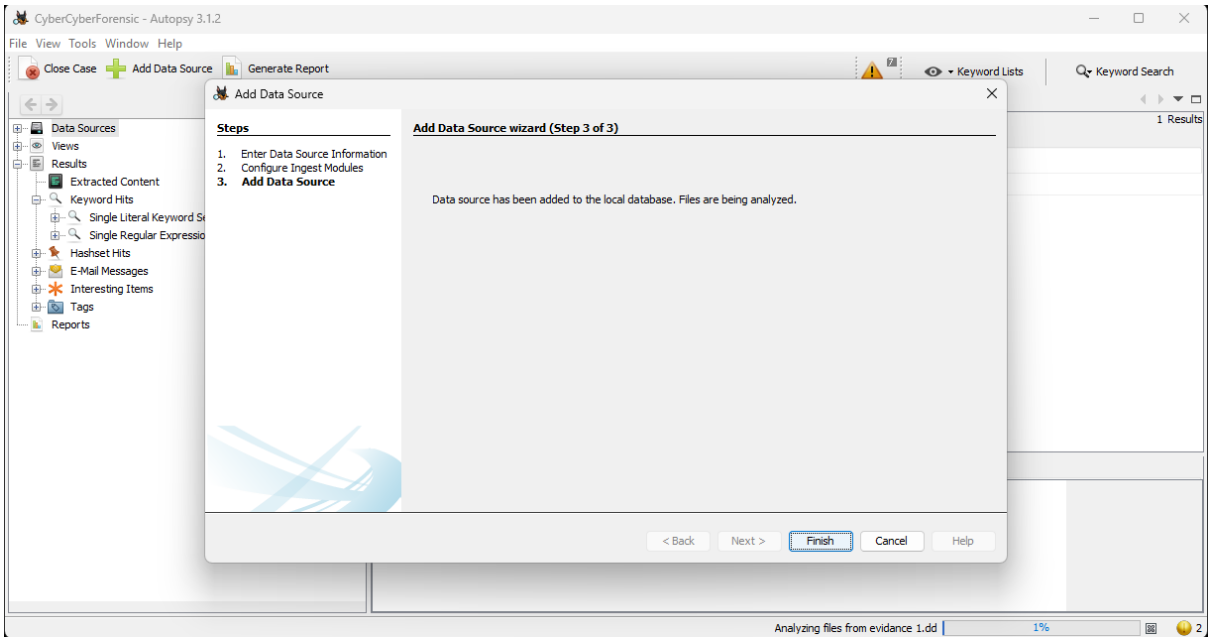
- **Click on Next**



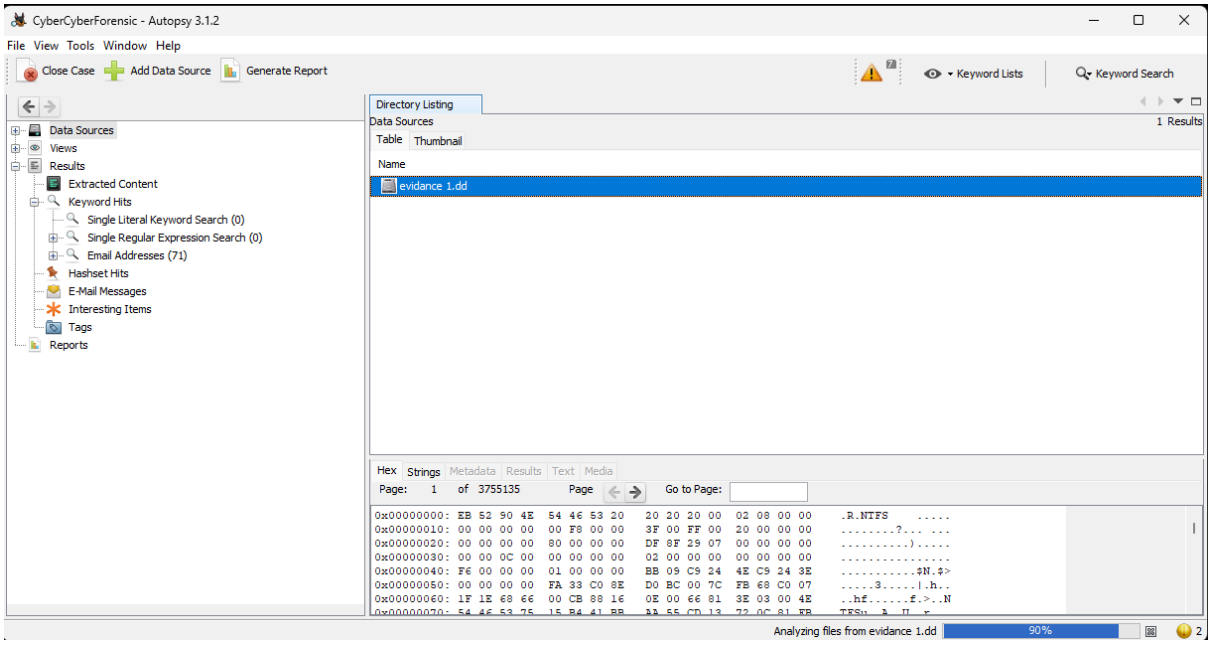
Step 5: In **configuration Ingest Modules Keep Default Setting** and **Click on Next**



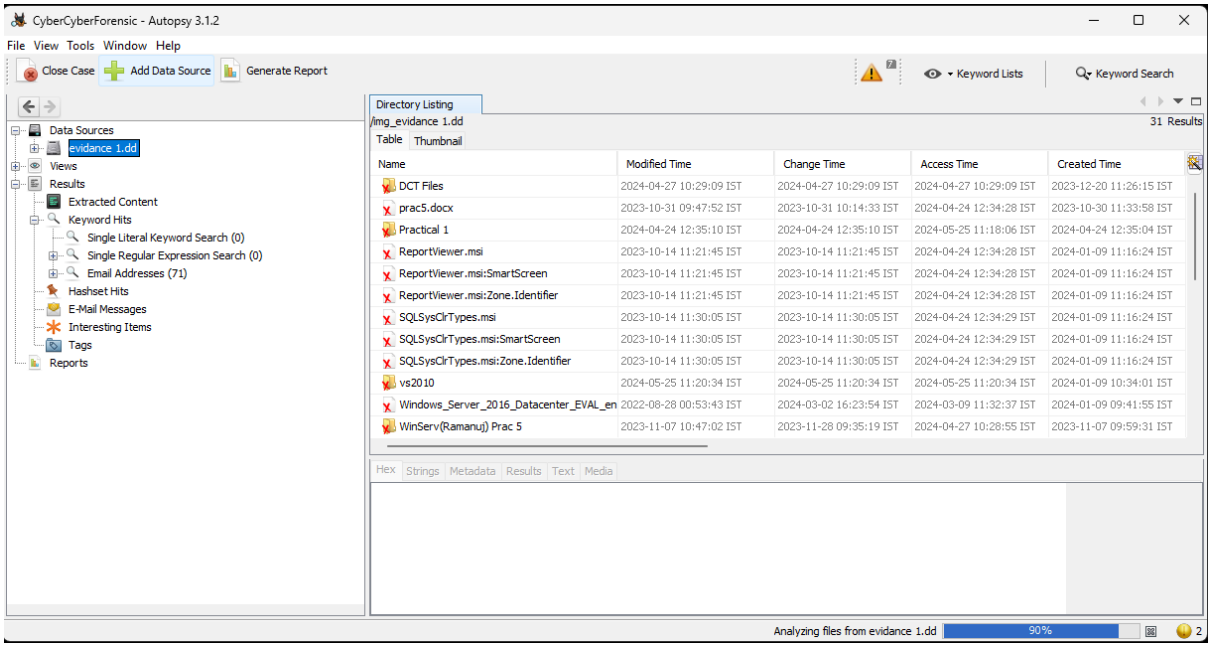
Step 6: Click on Finish



Step 7: It Analyzing the Files From evidence 1.dd

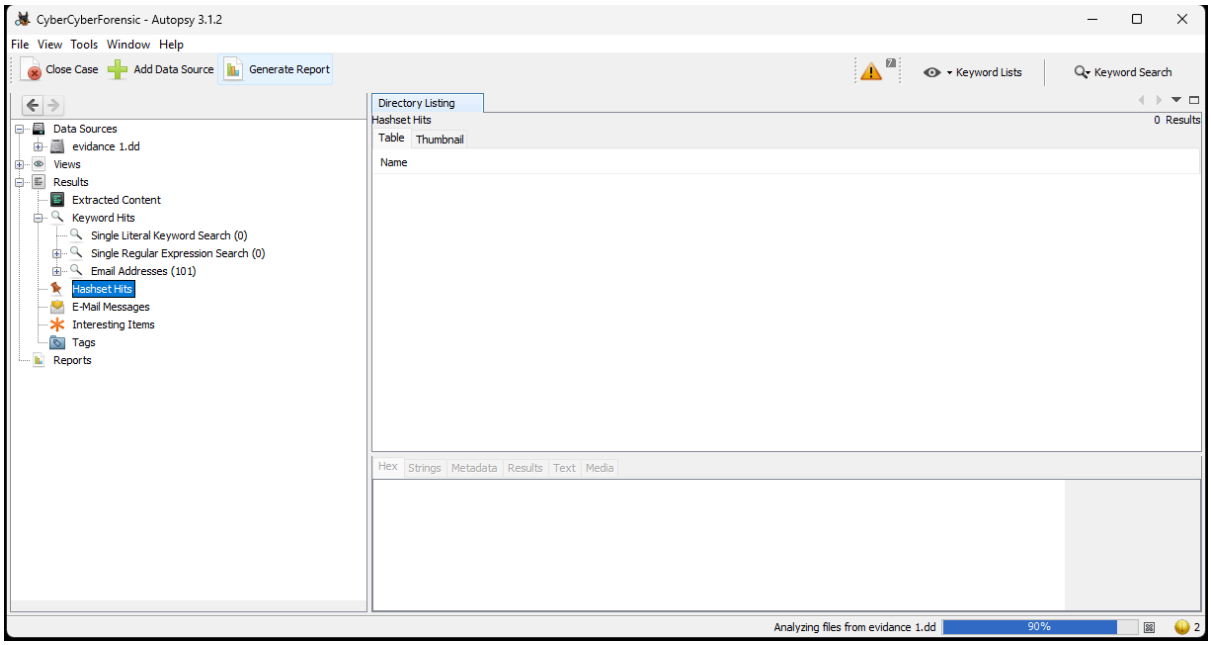


Step 8: Expand the Data Source there is one Hard Drive under Data Source Called evidence 1.dd by selecting evidence 1.dd we can see file structure or files in main view in the main view we can see the file name special attribute modified time change time access time.

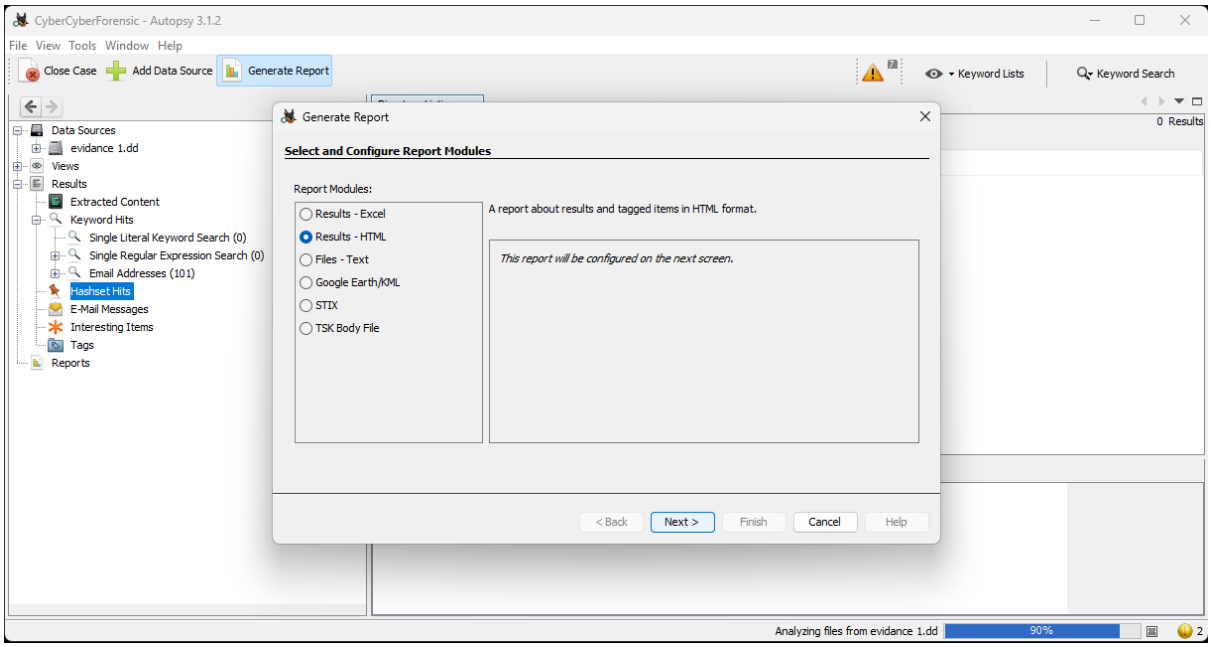


Step 9: After the image is indexed the tree will be populated by the file system, extracted content, keyword searches, and the hash list (if any were used). the investigator should generate a report. This will allow the investigator to have an idea of what type of information is available and what to expect. The report can be generated in three formats: Excel, XML, and HTML.

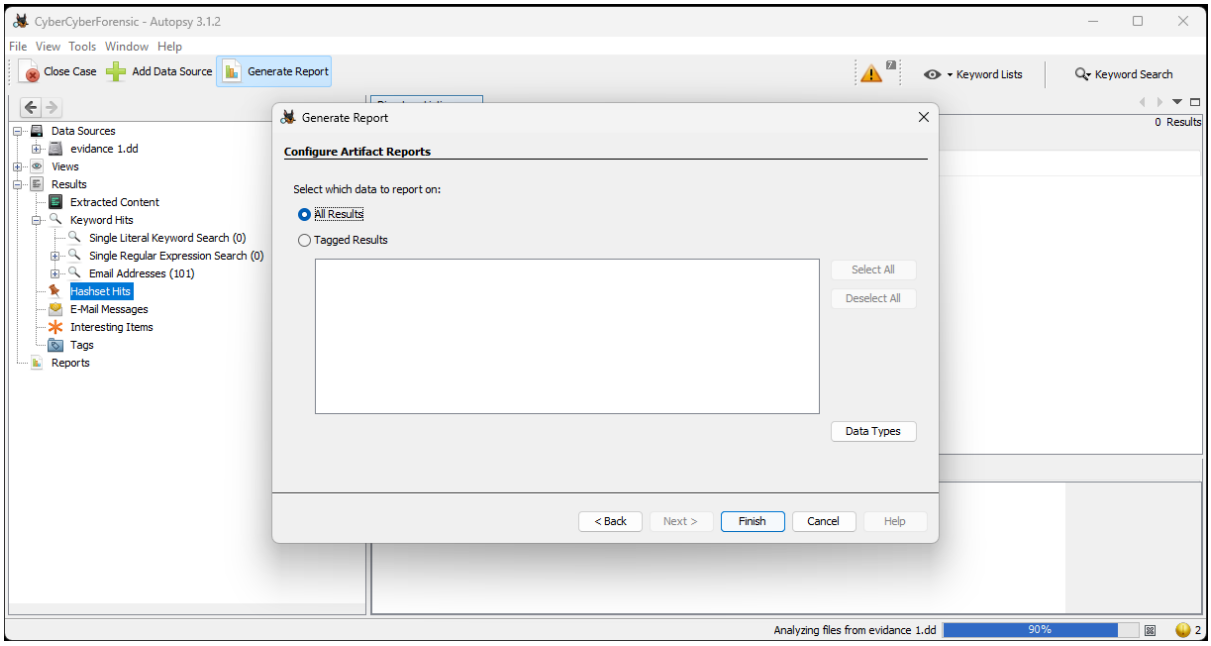
- **Click on Generate Report**



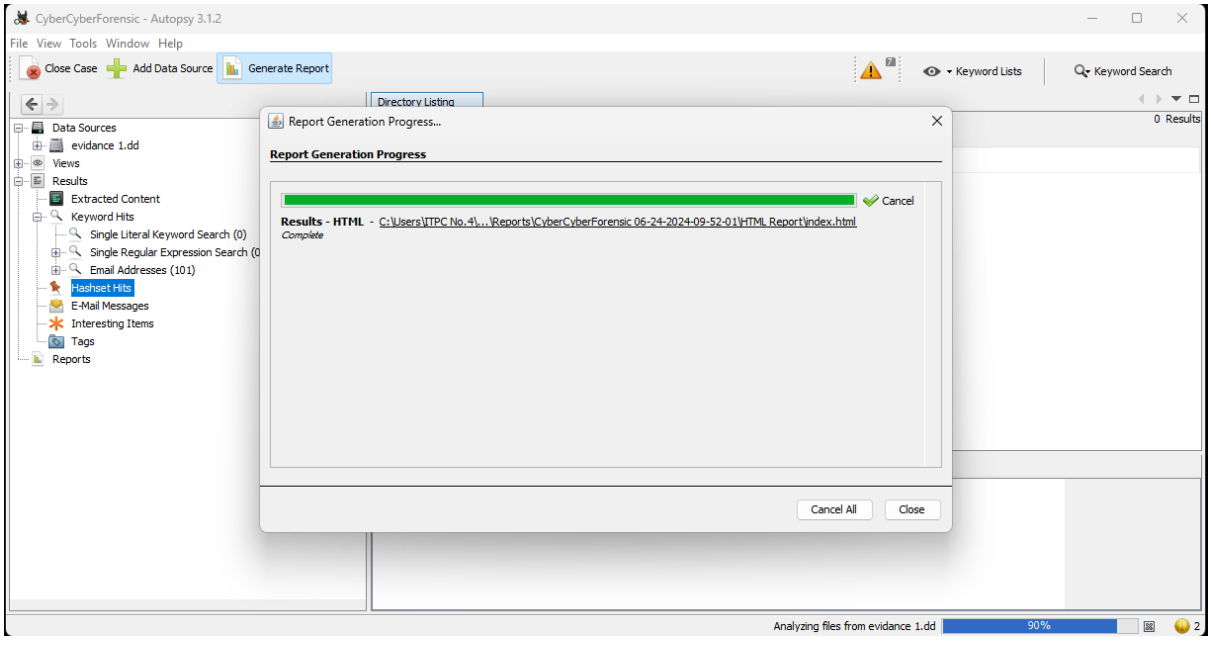
- **Select Result-HTML** and **Click on Next**



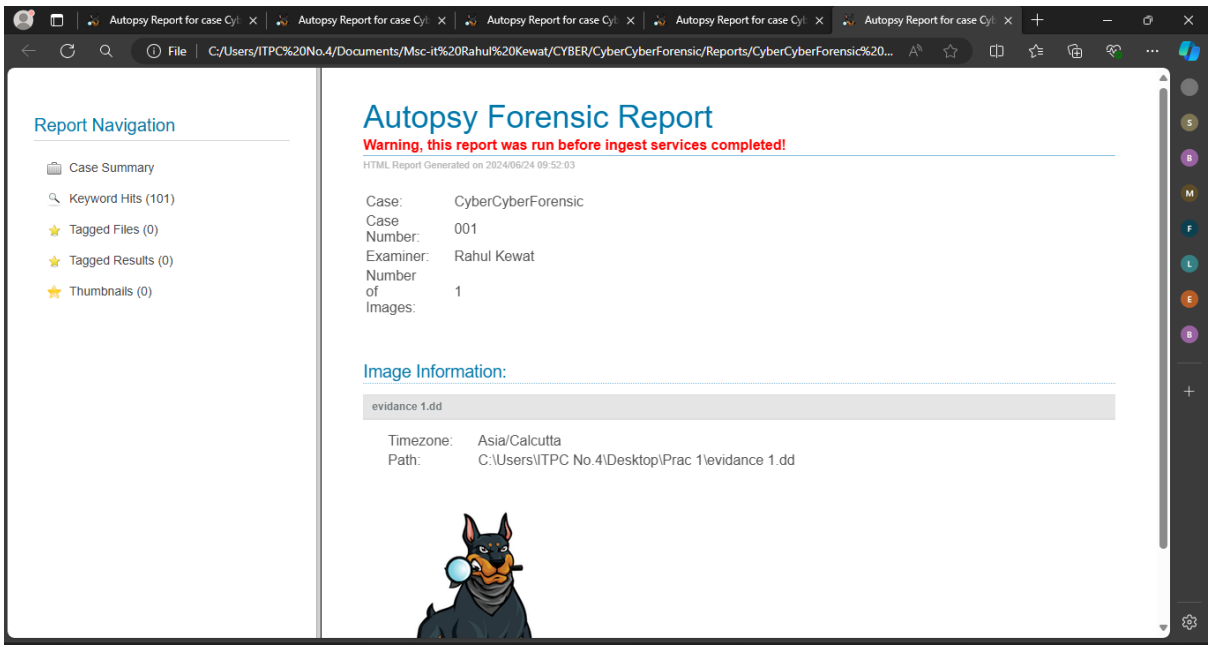
- **Select All Results** and **Click on Finish**



- Report Generation in Progress After Completion Click on Given link to view the Report

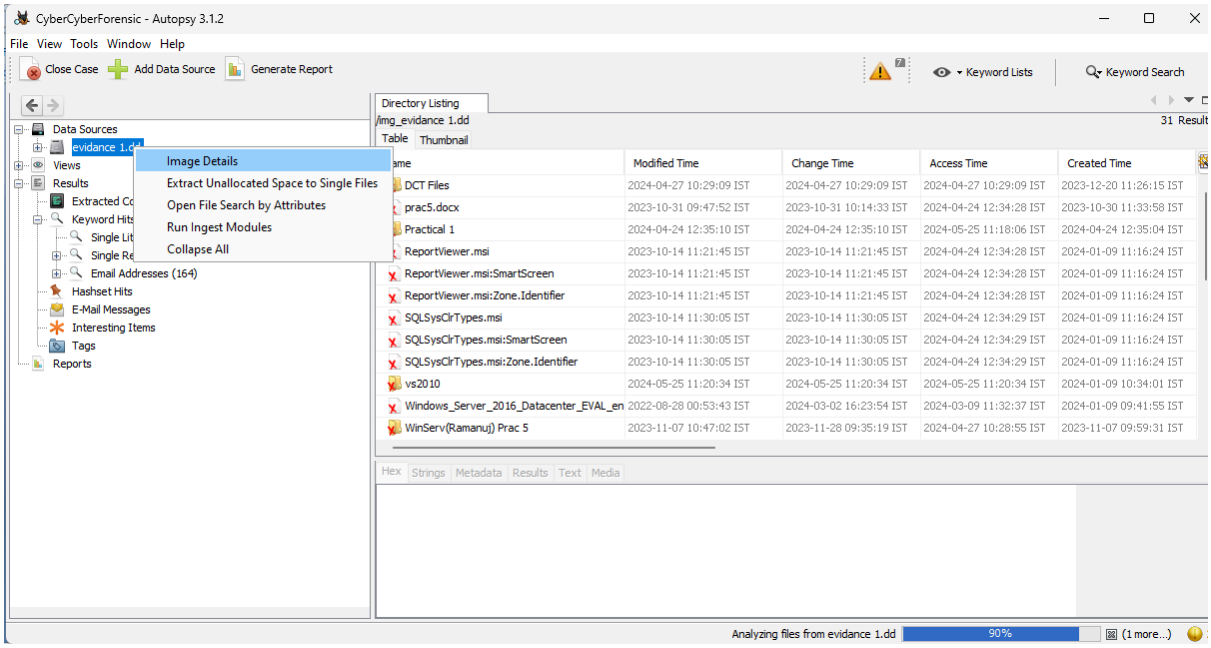


- Report Generated

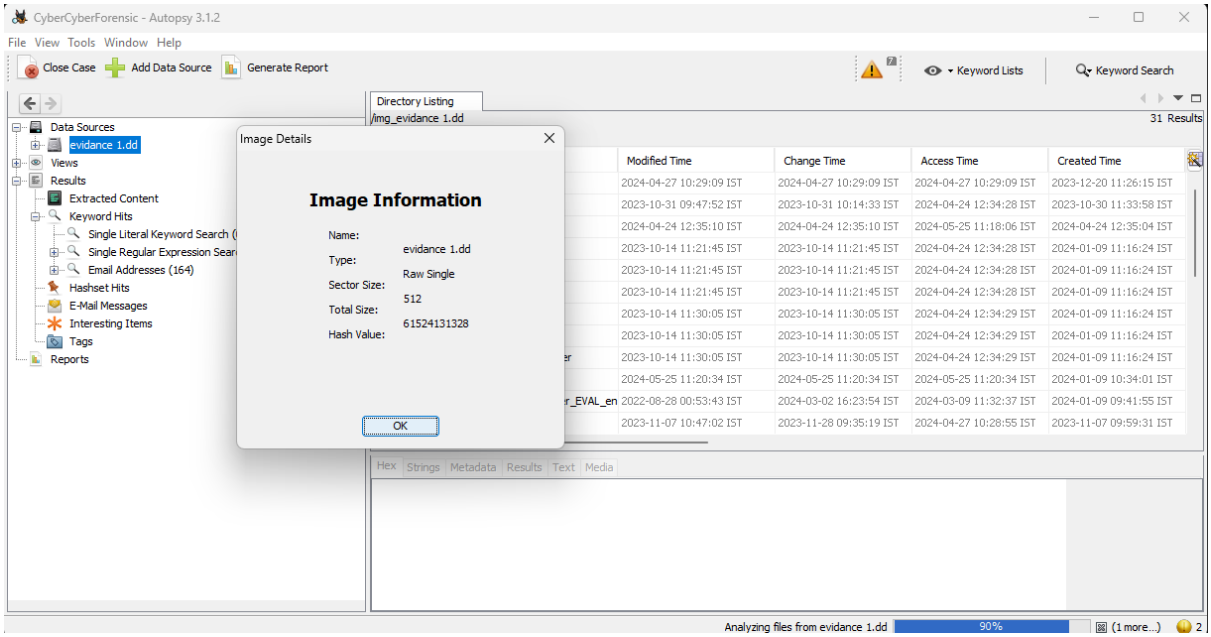


Step 10: View image detail

- **Right-Click on evidence 1.dd** and **Select image Details**



- **Here we can see Image Information**

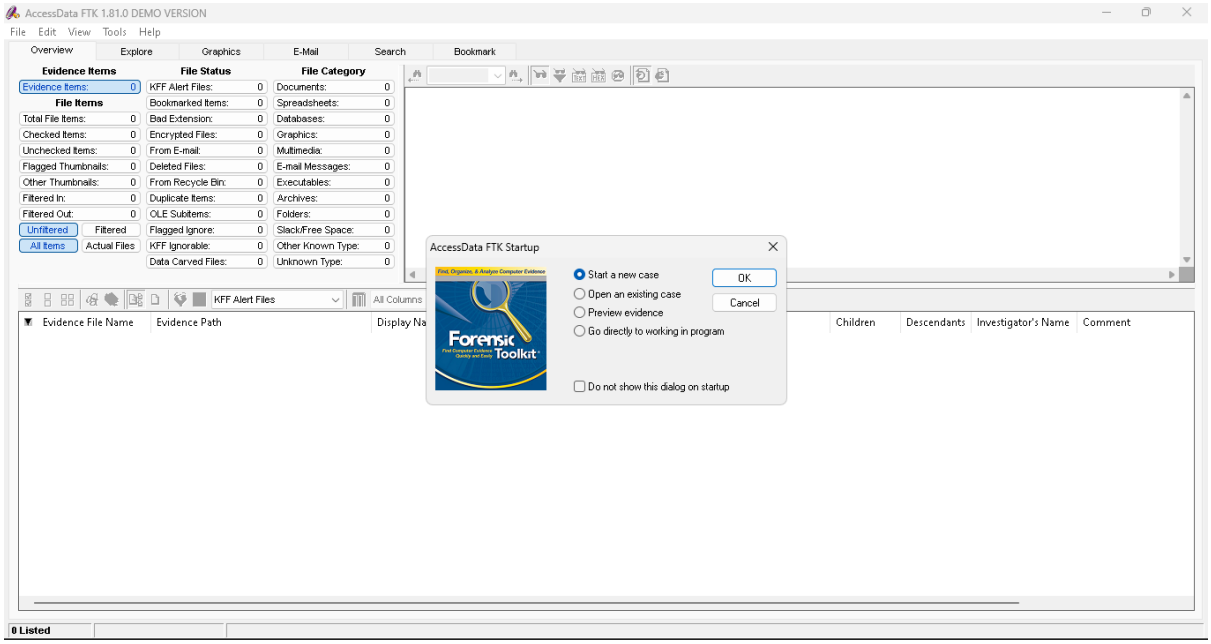


Practical: 2

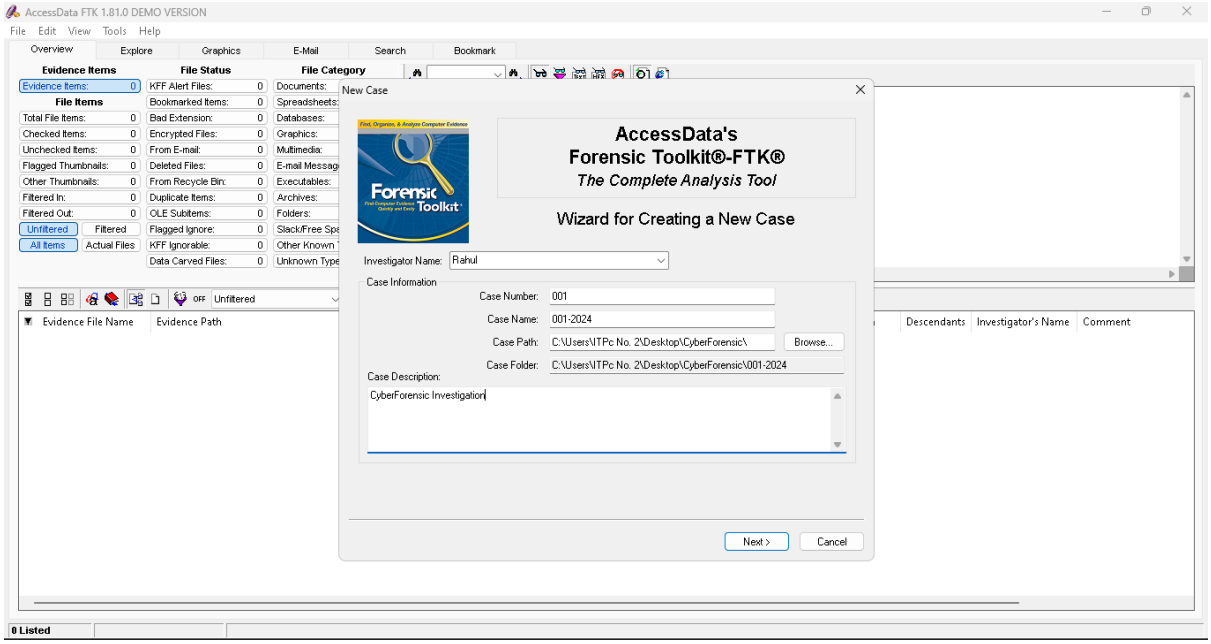
Aim: Using Forensic Toolkit (FTK) &Writing report using FTK (AccessData FTK).

Writeup:

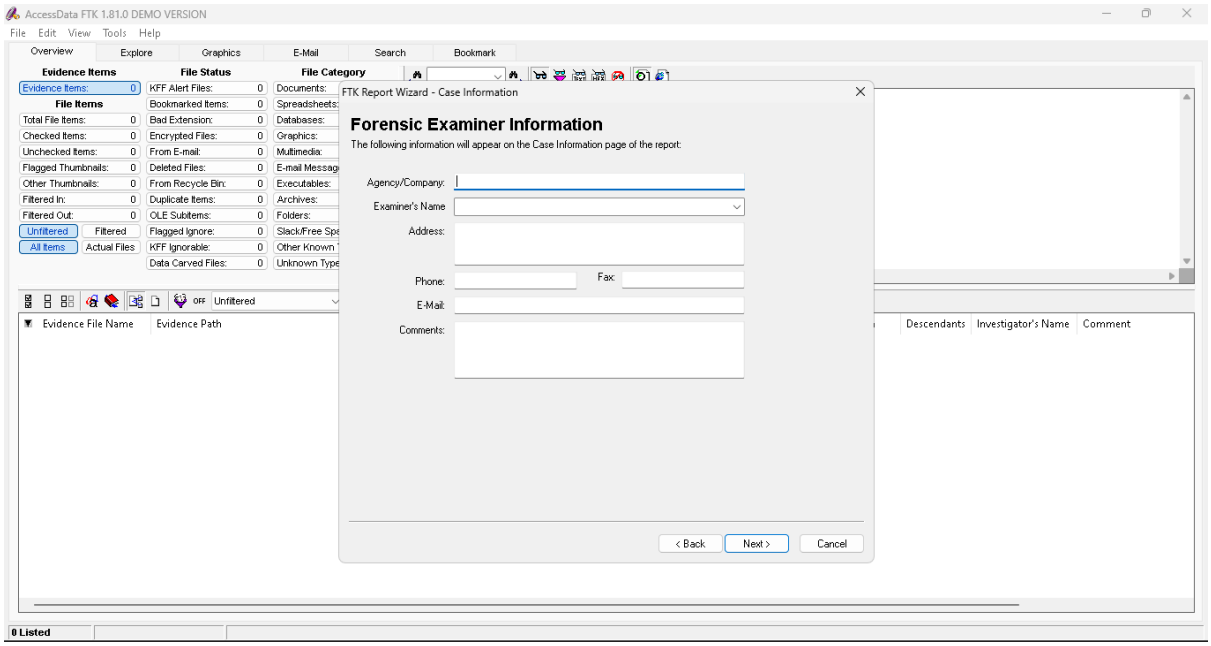
Step 1: Open **AccessData FTK 1.81.0 DEMO VERSION** and **Click on Start a new case** and **Click** on **OK**



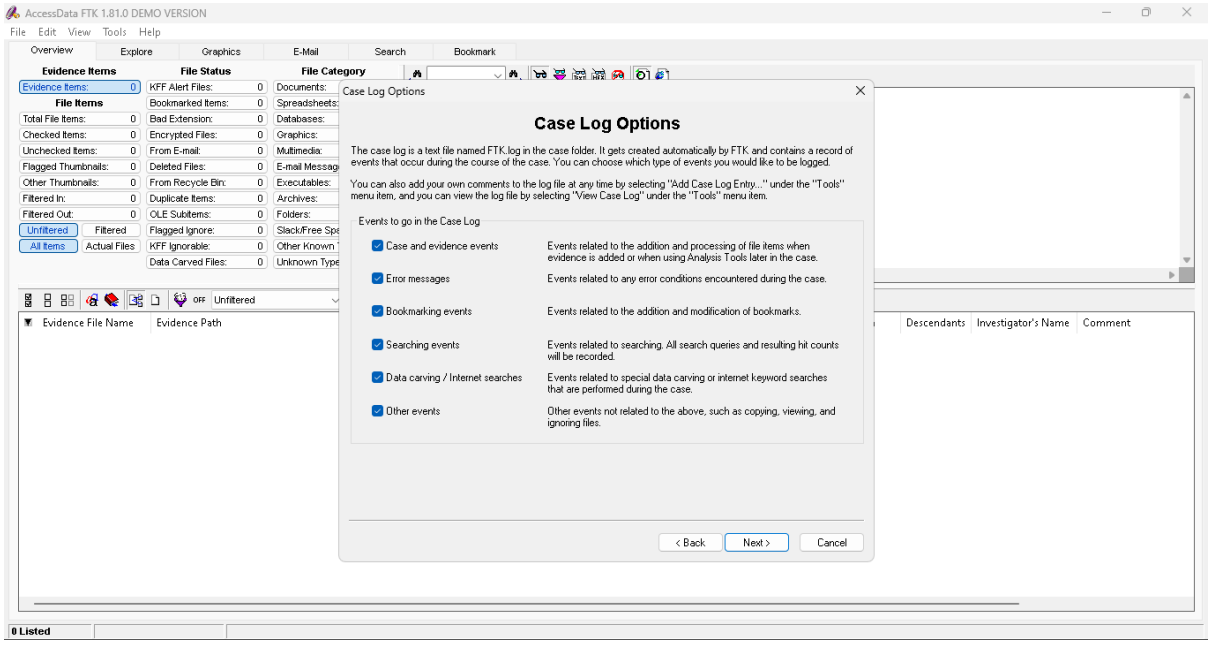
Step 2: Type **Investigator Name** and **Case Number, Case Name** and **Set** the **Case Path** and **Click on Next**



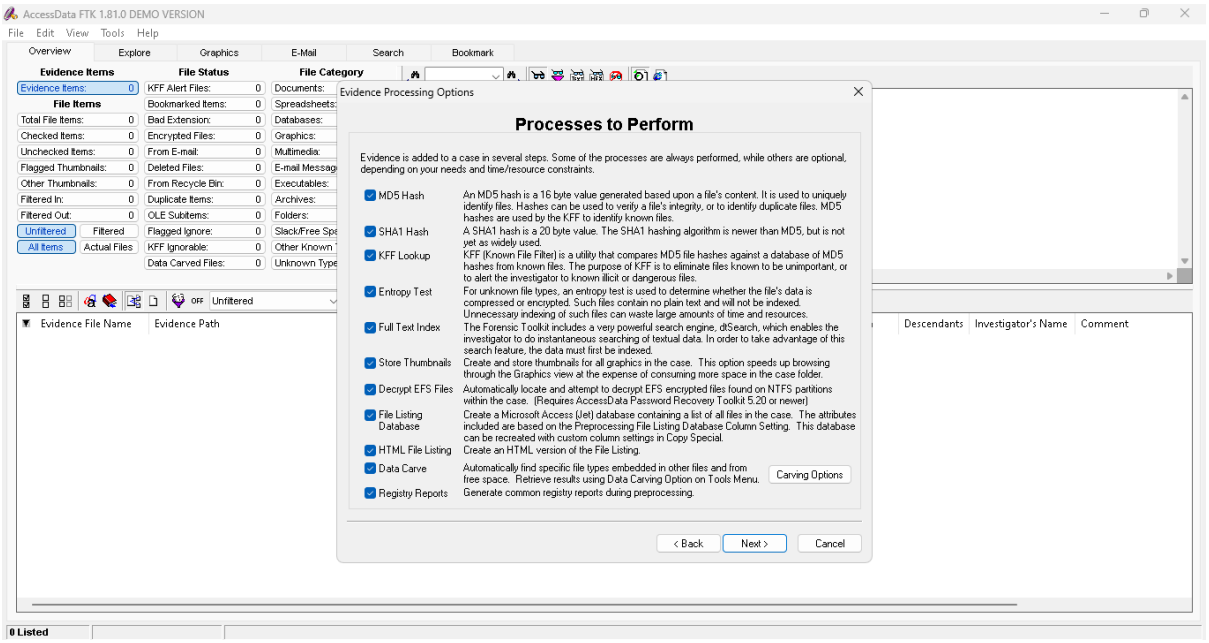
Step 3: Keep Default Setting and **Click on Next**



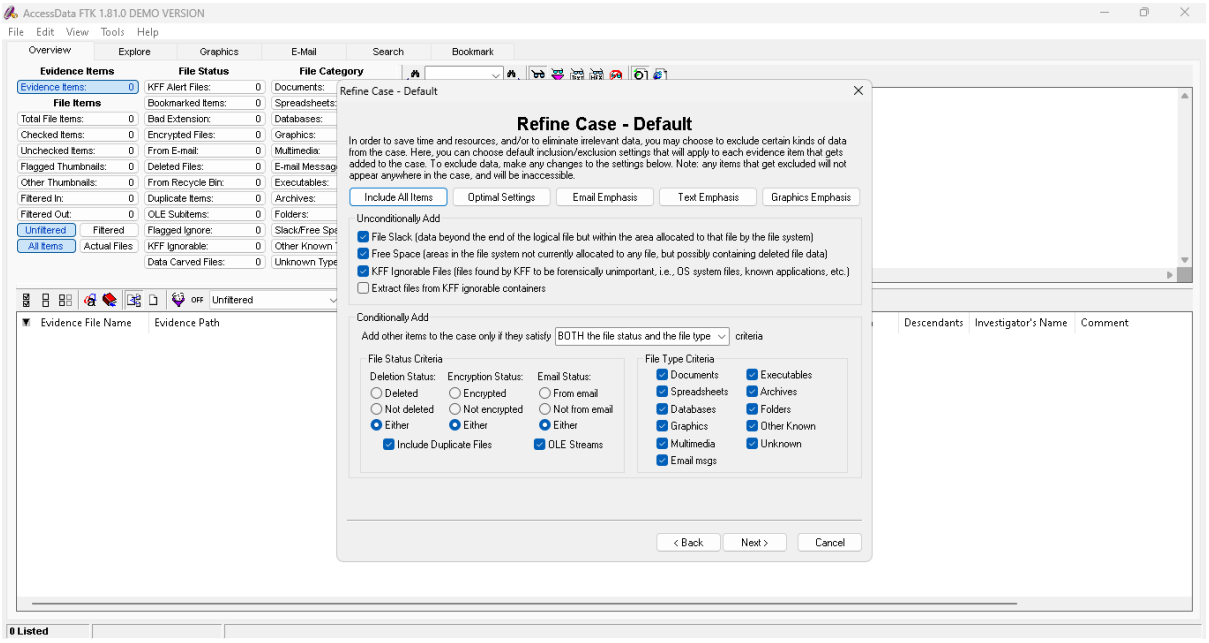
Step 4: Keep Default Setting and **Click on Next**



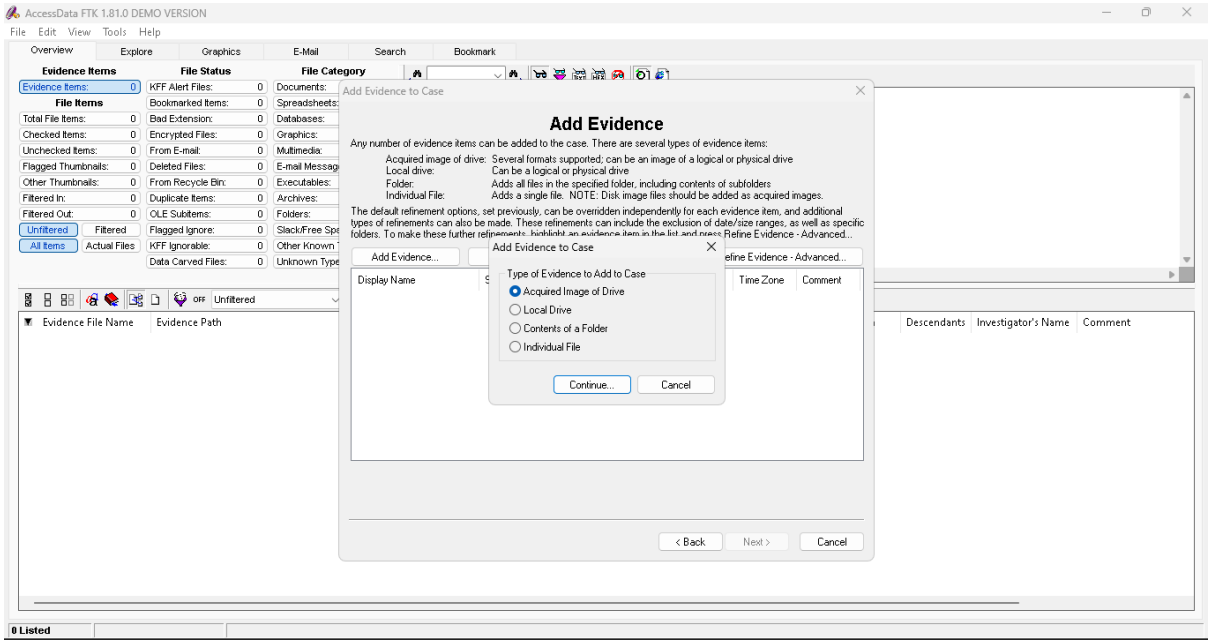
Step 5: Select Data Carve and Registry Report and Click on Next



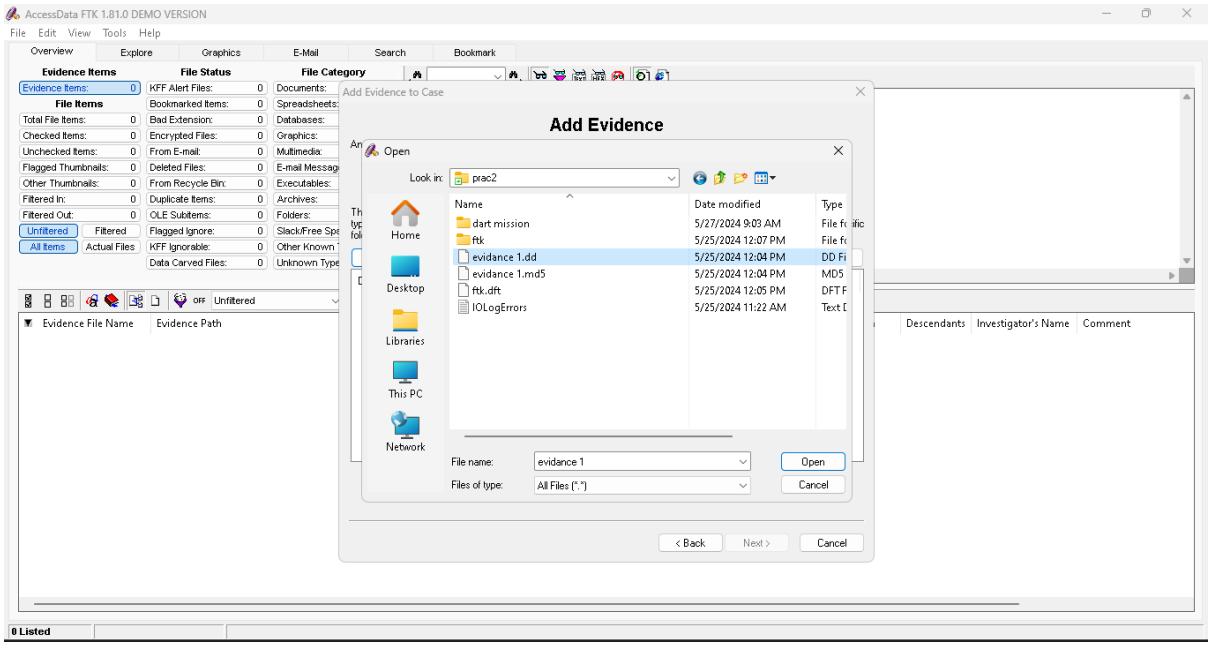
Step 6: Keep Default Setting and Click on Next



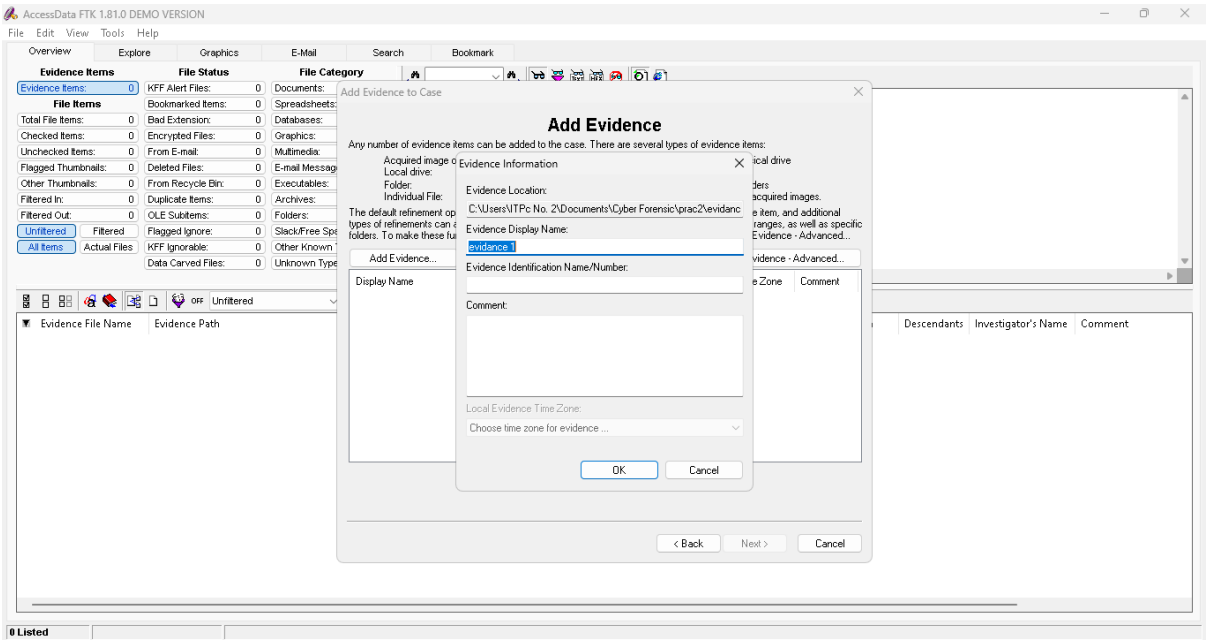
Step 7: Click on Add Evidence Within Type of Evidence to Add to Case Select Acquired Image of Drive and Click on Continue



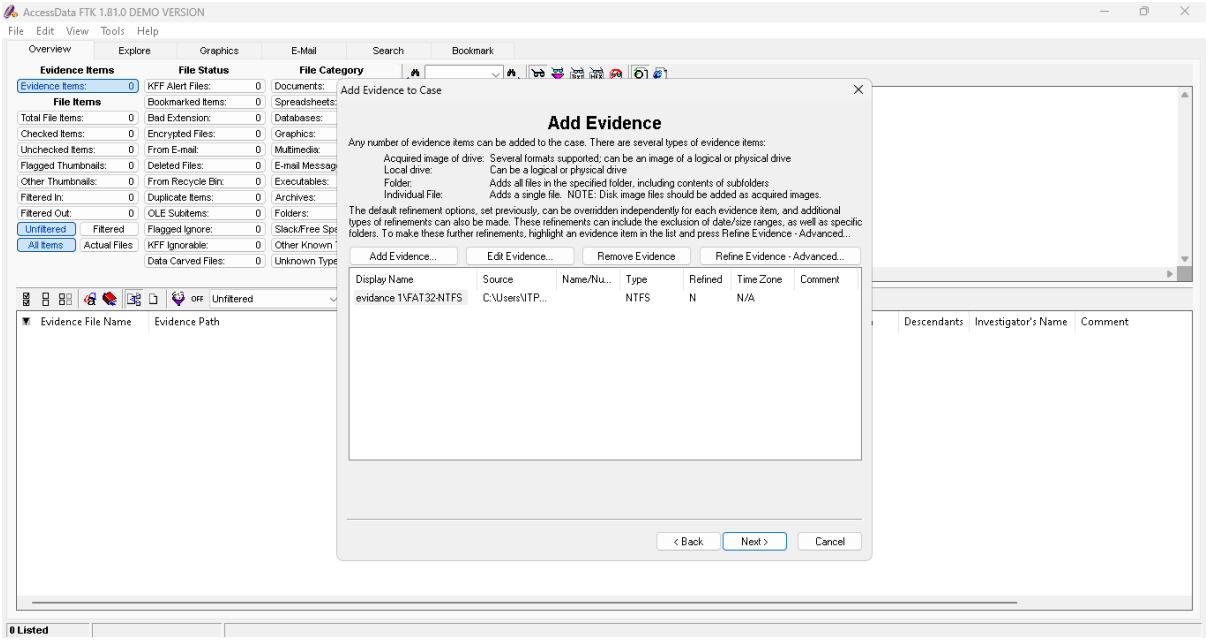
- **Within Add Evidence Select evidence 1.dd and click on open**



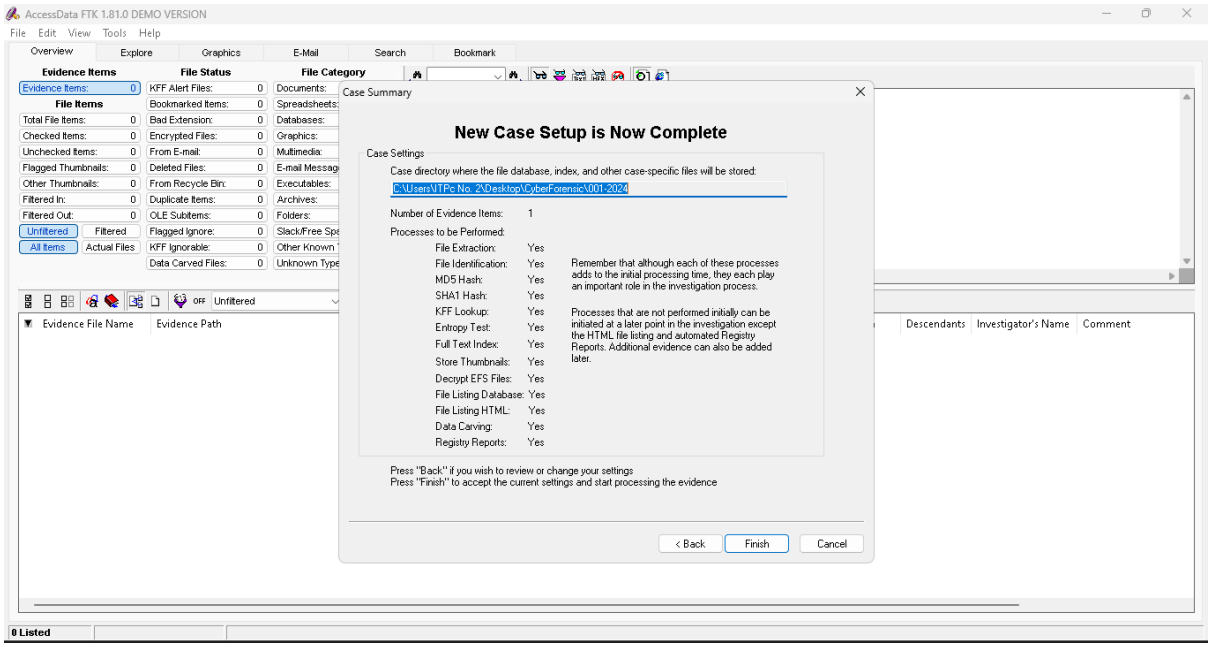
- **Click on OK**



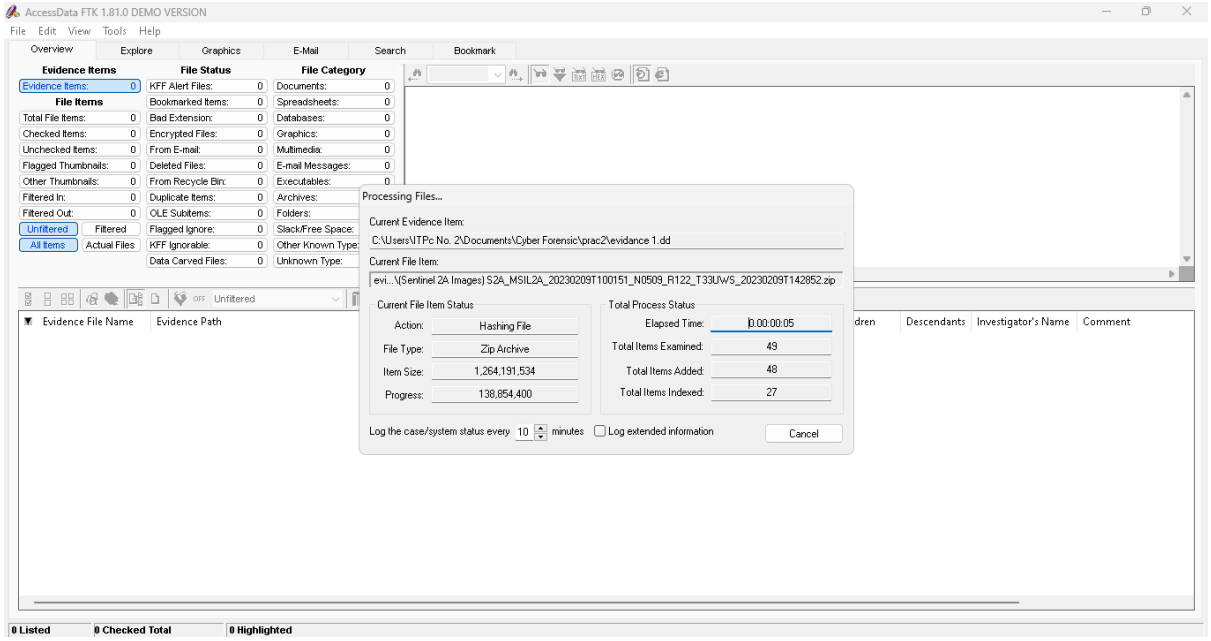
- **Click on Next**



- **Click on Finish**

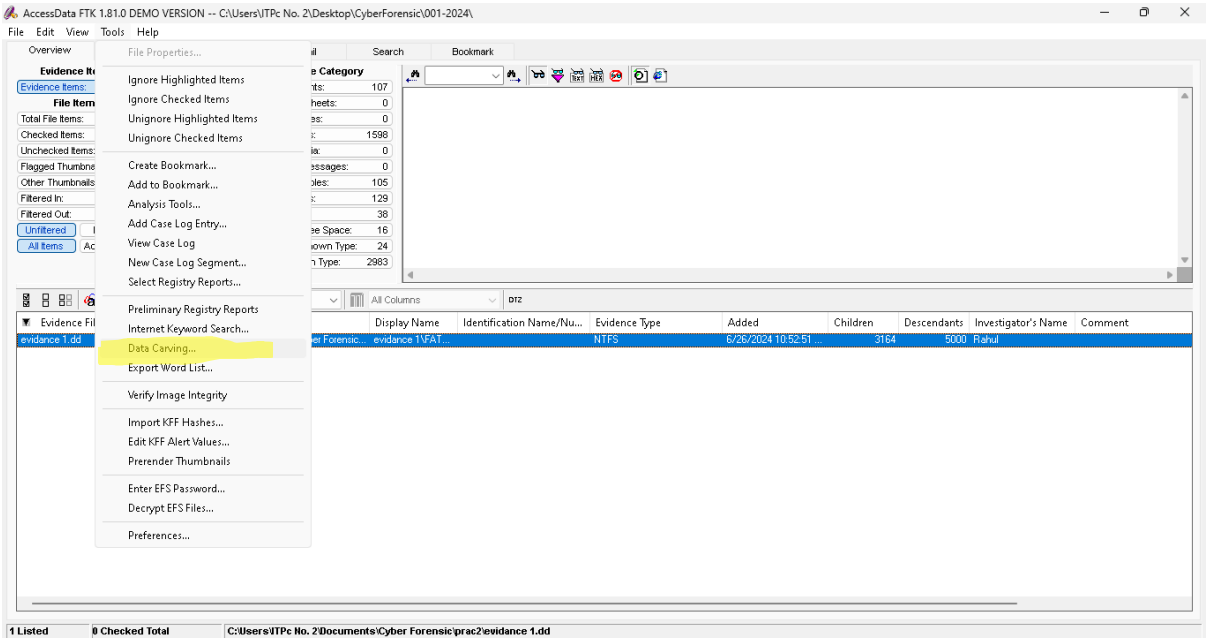


- It Start the Processing Files

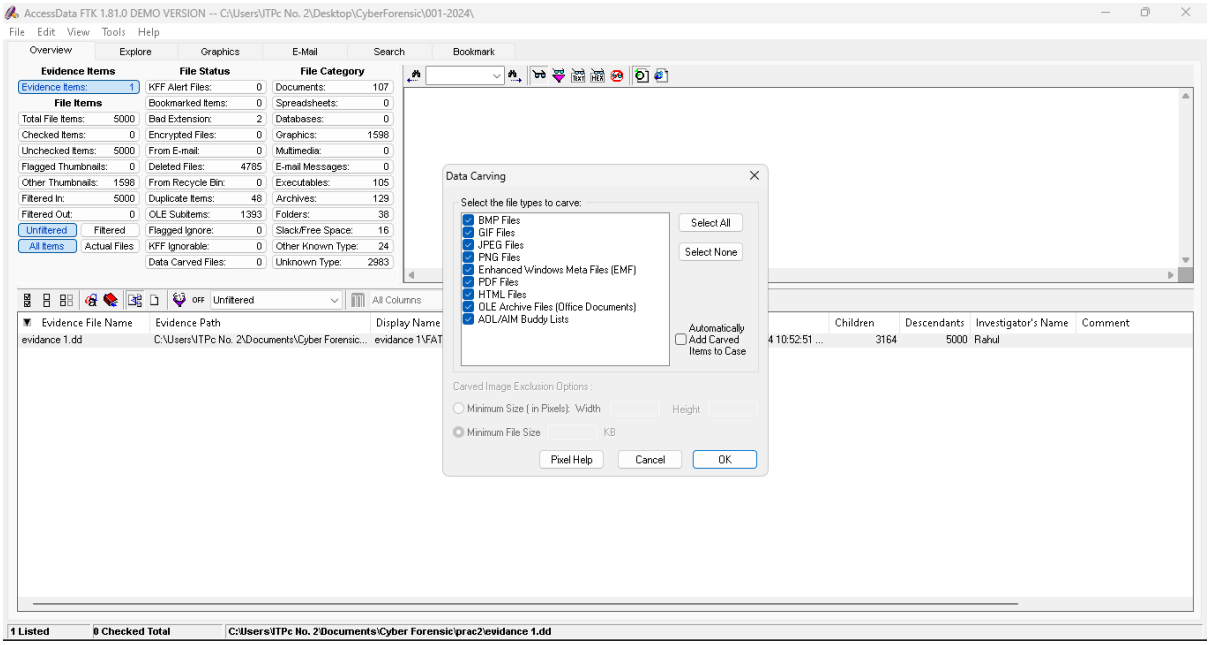


Step 8: Data Carving Files in an Existing Case

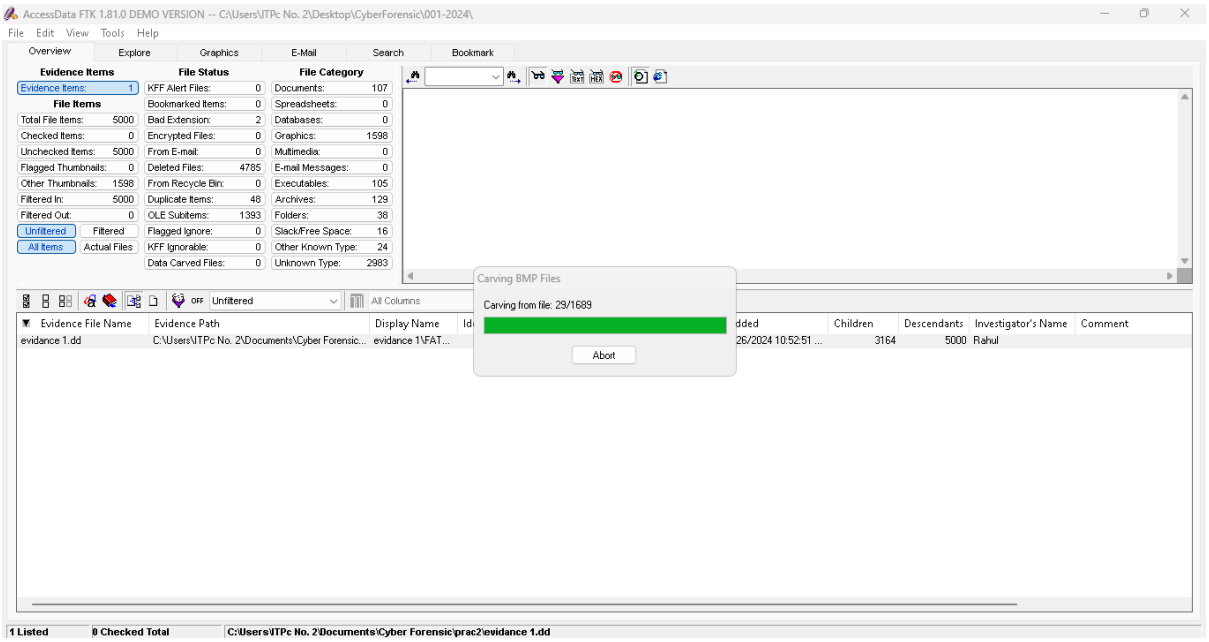
- **Select Tools,** and then **Data Carving.**



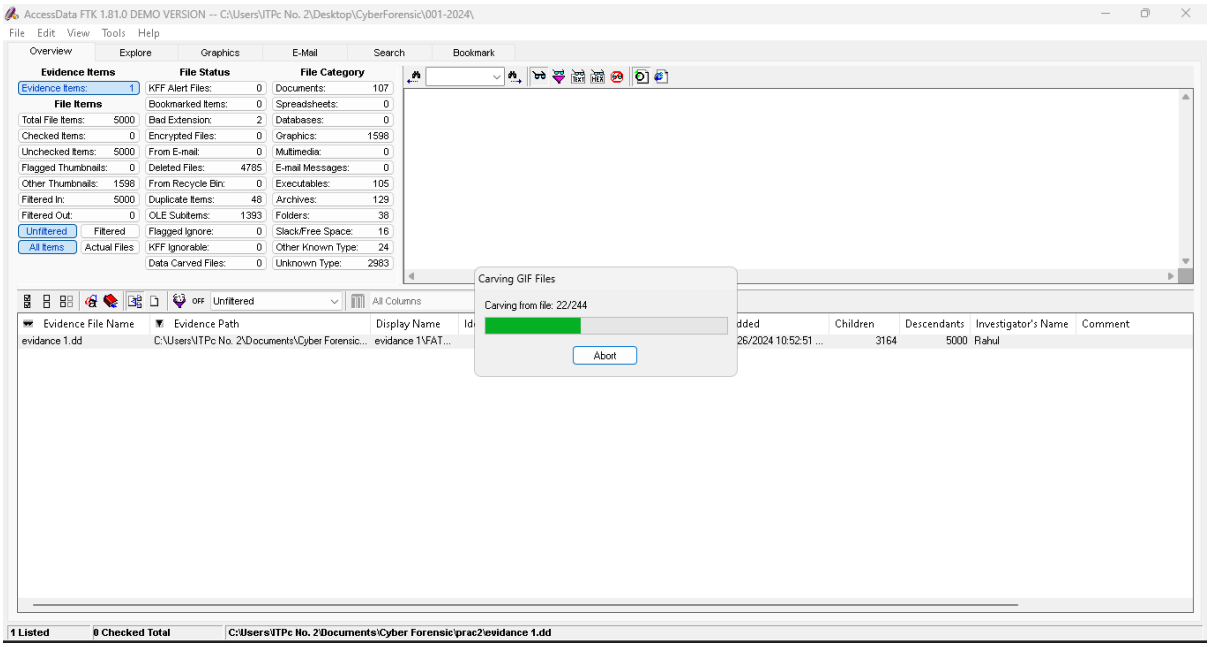
- **Select BMP Files, GIF Files,** and **PNG Files** and **Click on OK**



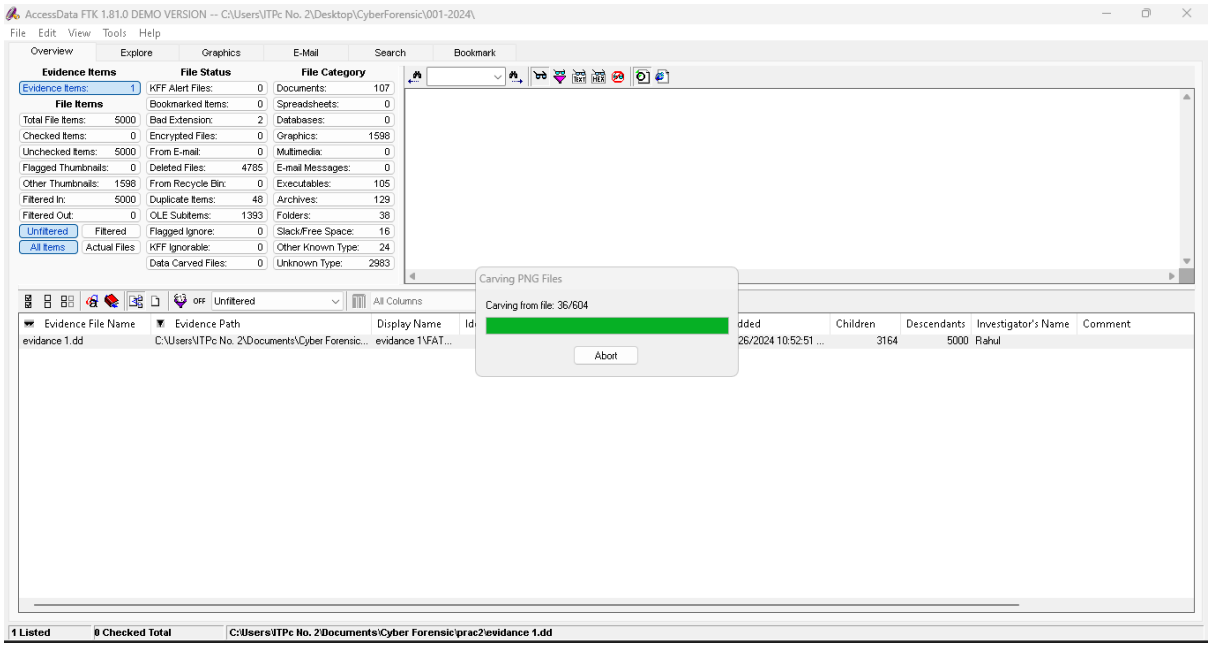
- It Will Start Carving BMP Files



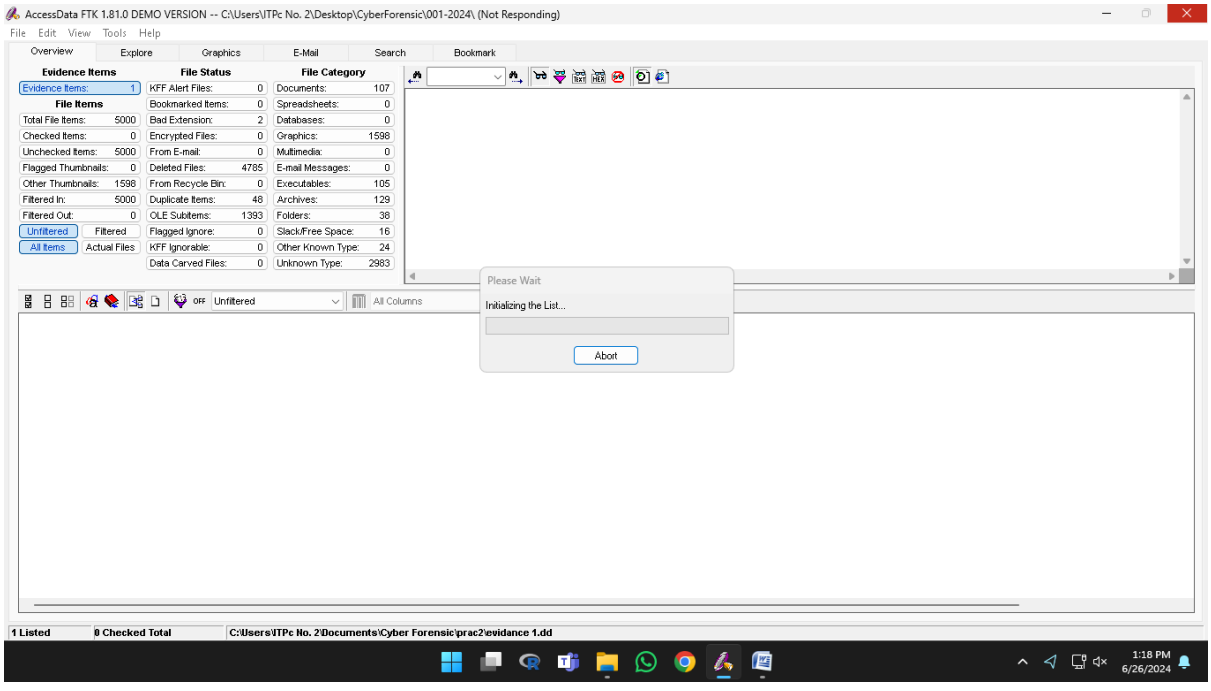
- After Carving BMP Files It Will Start Carving GIF Files



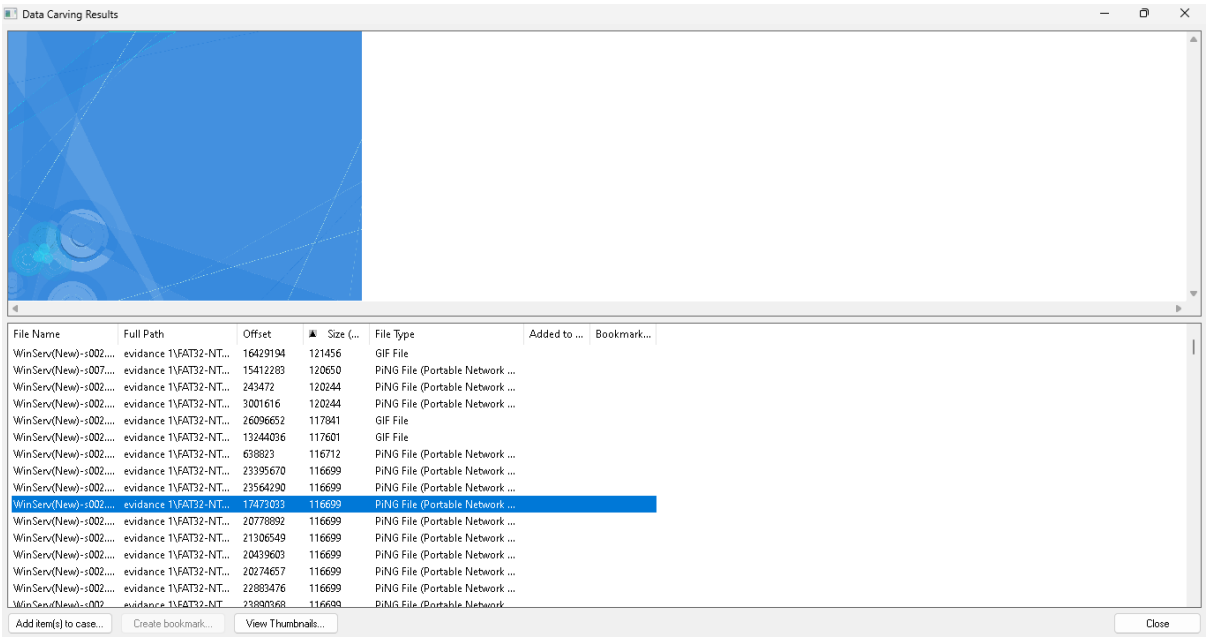
- After Carving BMP and GIF Files and then Next It Will Start Carving PNG Files



- After Carving BMP and GIF, PNG Files and then Next It Will Start Initializing the list

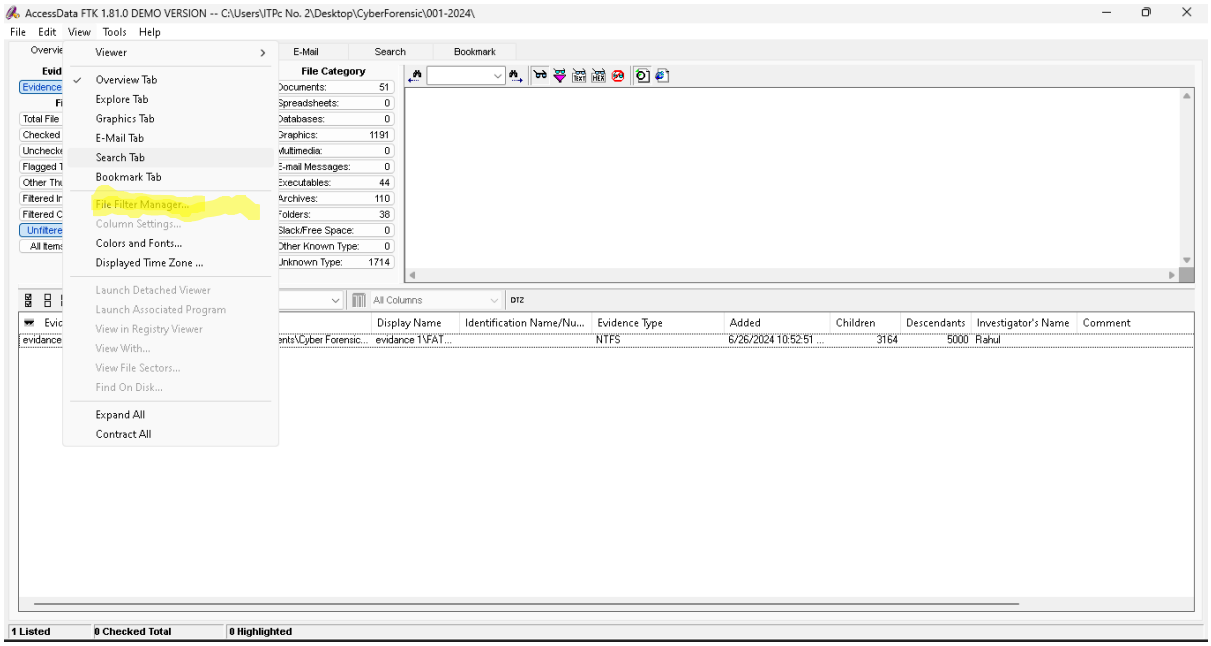


- After Initializing the list Here, We Can See the **Data Carving Results**

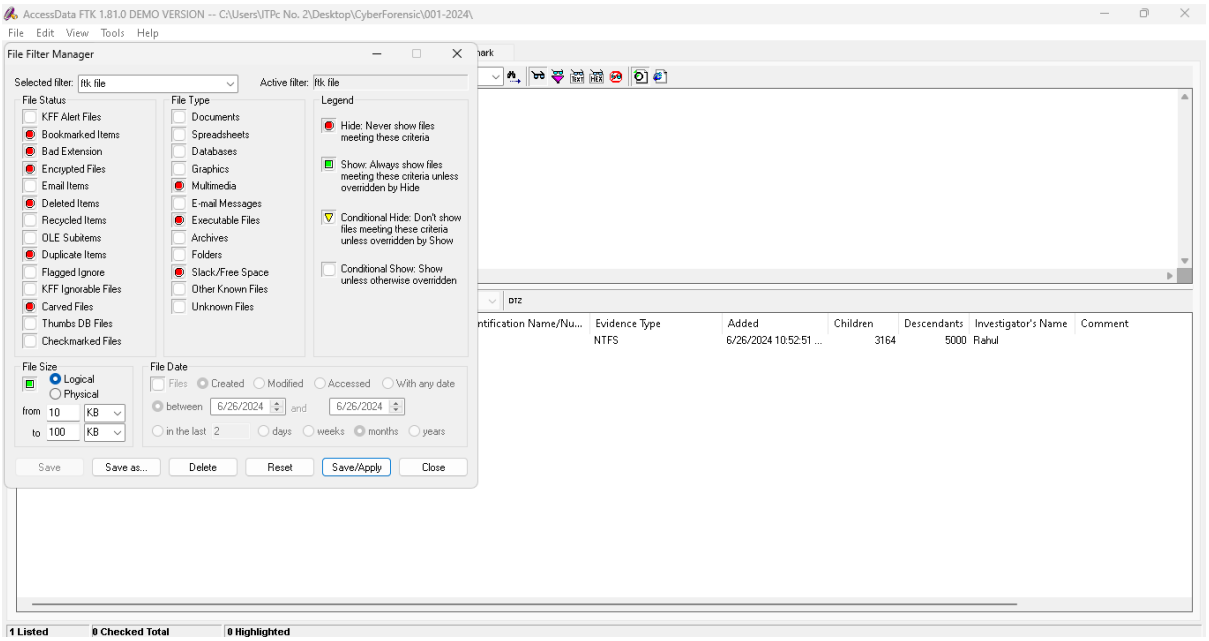


Step 9: Modifying or Creating a Filter

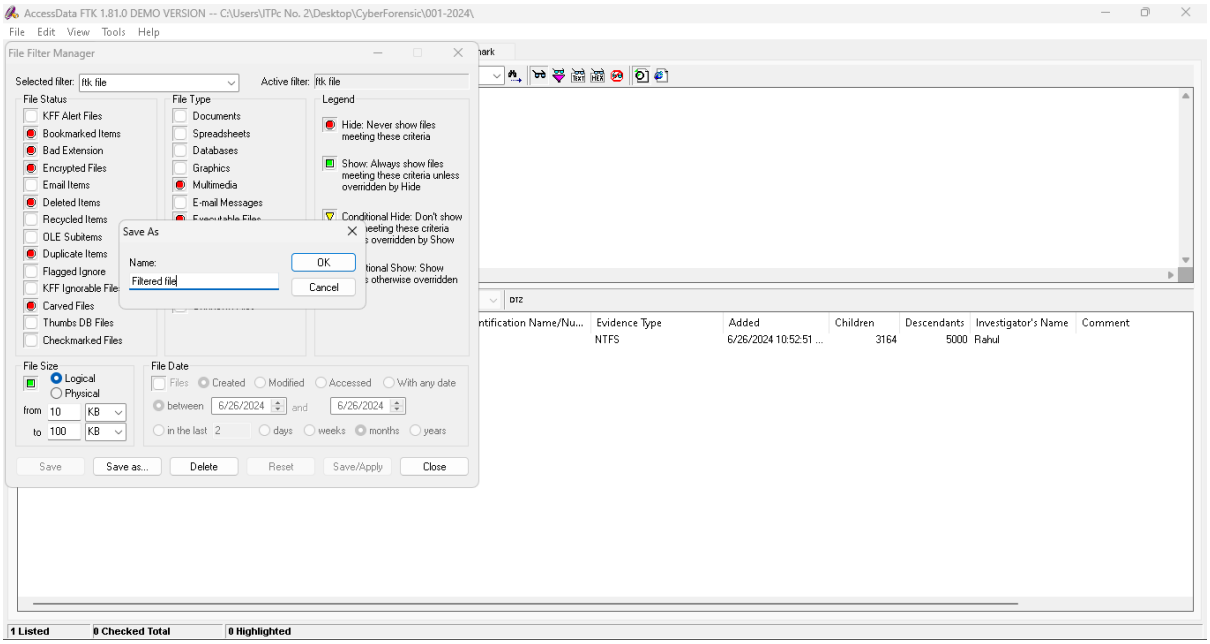
- **Select View,** and then **File Filter Manager**



- Select the filter that you want to modify

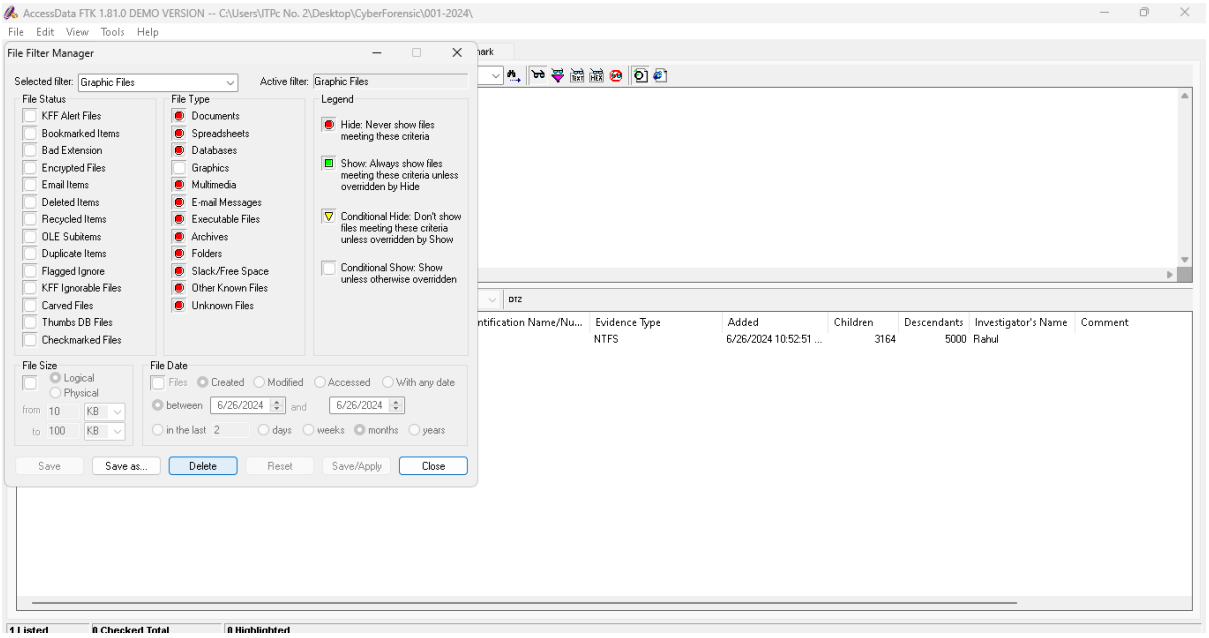


- If you are modifying an existing filter, **click Save/Apply.** Or If you are creating a new filter, **click Save As,** enter the name, and **click OK.**

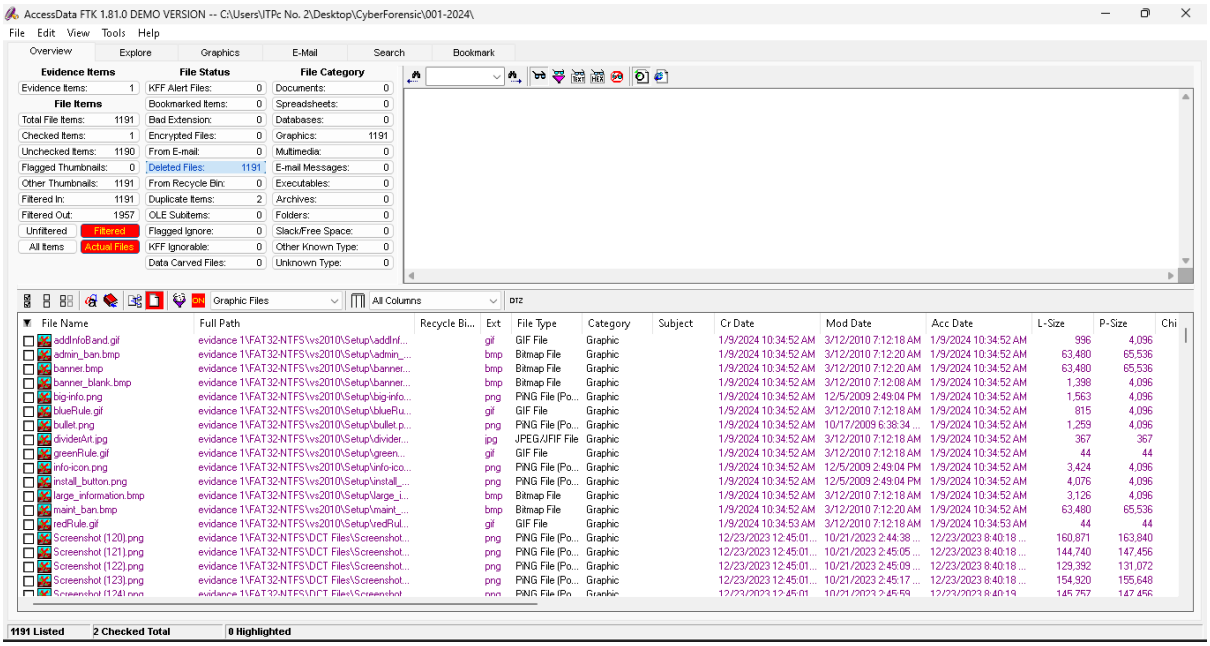


Step 10: Deleting a Filter

- You can delete a filter if you no longer need it. To delete a filter:
- **Select View**, and then **File Filter Manager.**
- **Click Delete**

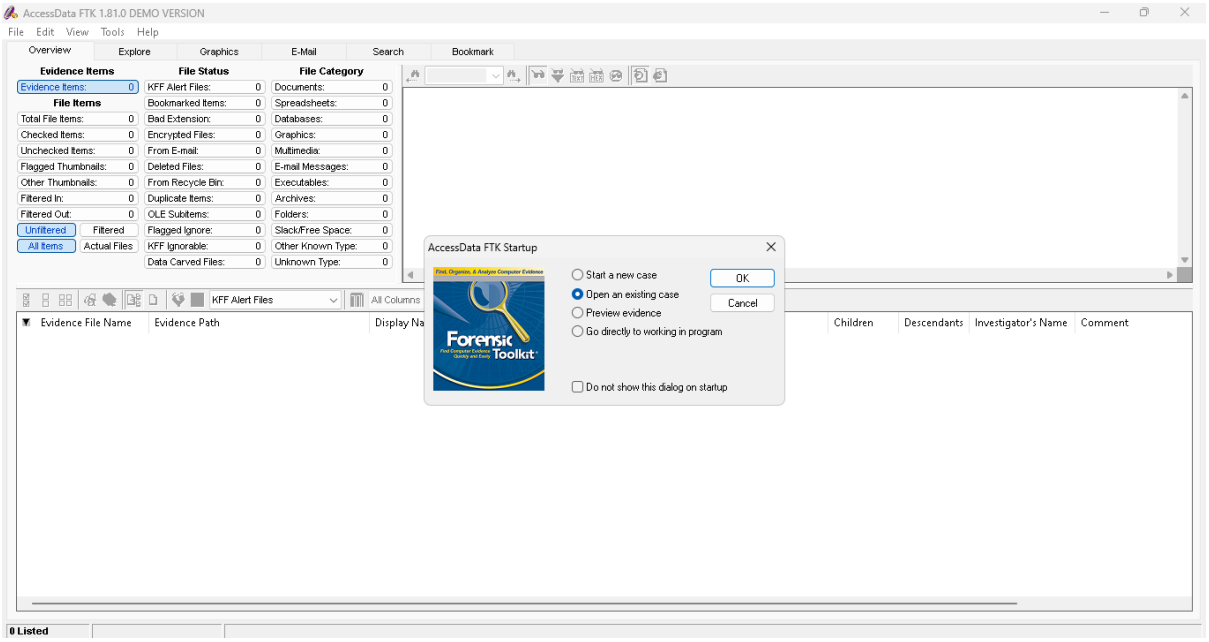


- Deleted Files

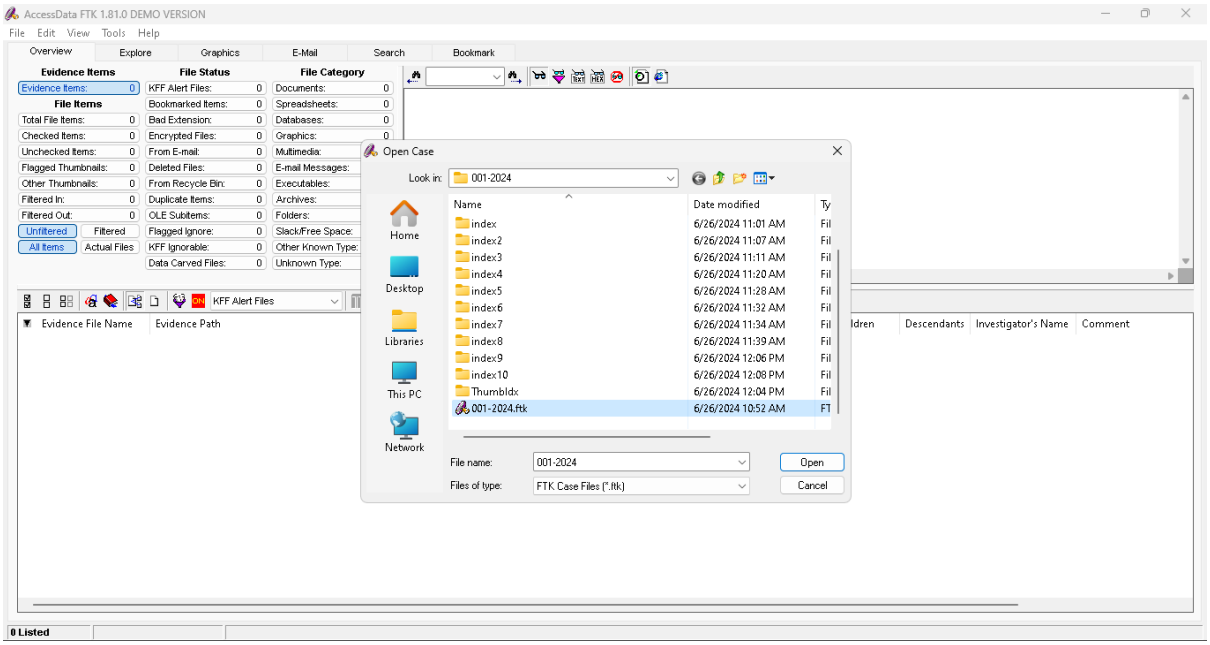


Step 12: Searching the Registry

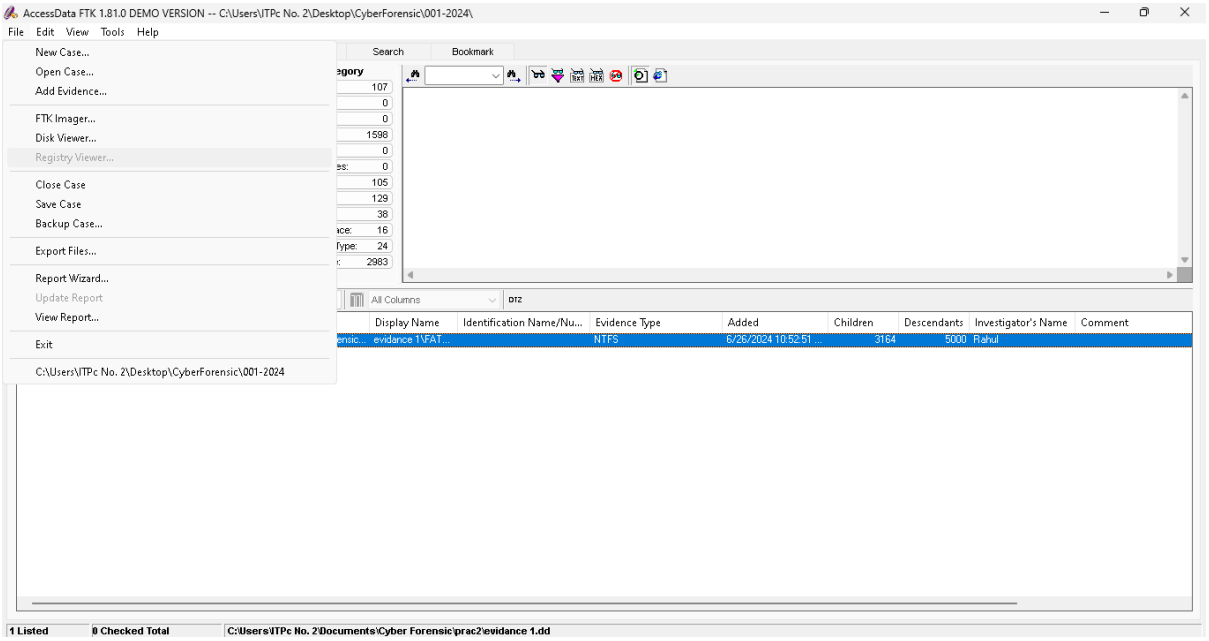
- **Launching Registry Viewer** as a Separate Application:
- To run Registry Viewer as a separate application, select Start, then Programs, then AccessData, and then Registry Viewer, and then Registry Viewer
- Launching Registry Viewer from FTK:
- To run Registry Viewer from FTK:
- In FTK, open an existing case by selecting File, and then Open Case.
- Or if you have chosen to always display the FTK Startup screen, select Open an Existing Case and click OK



- **Select** the case you want to open.

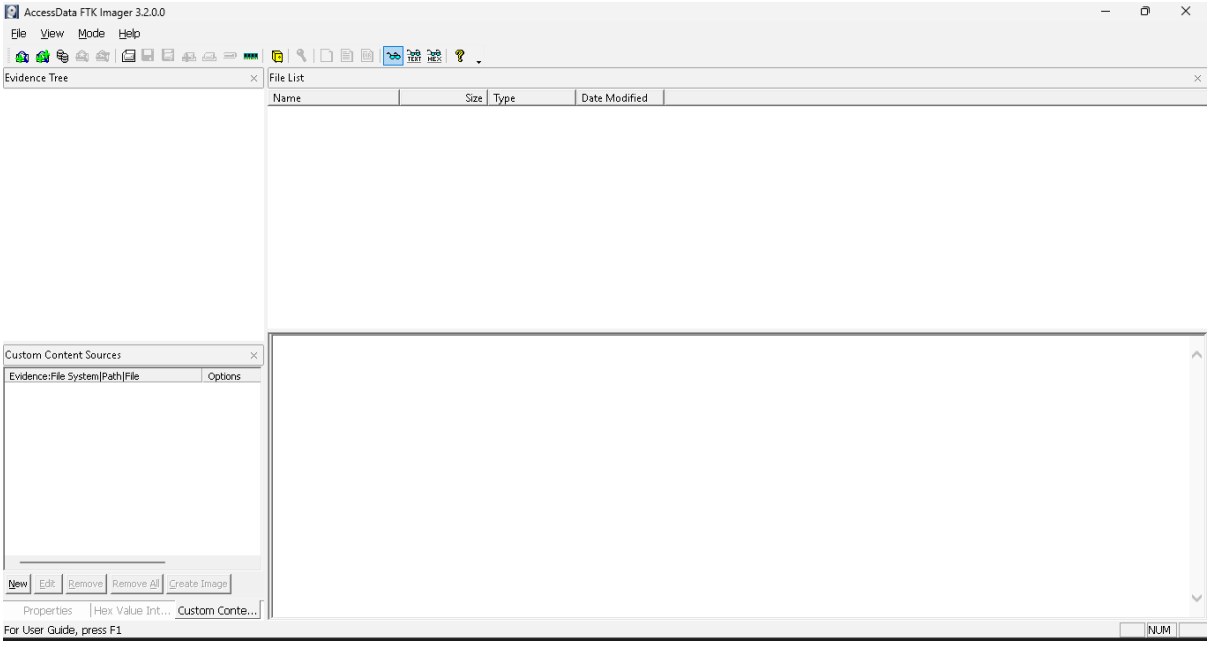


- **Select File,** and then **Registry Viewer** to **open Registry Viewer.**
- (Can't perform ahead of this step because Registry viewer is disabled in demo version)

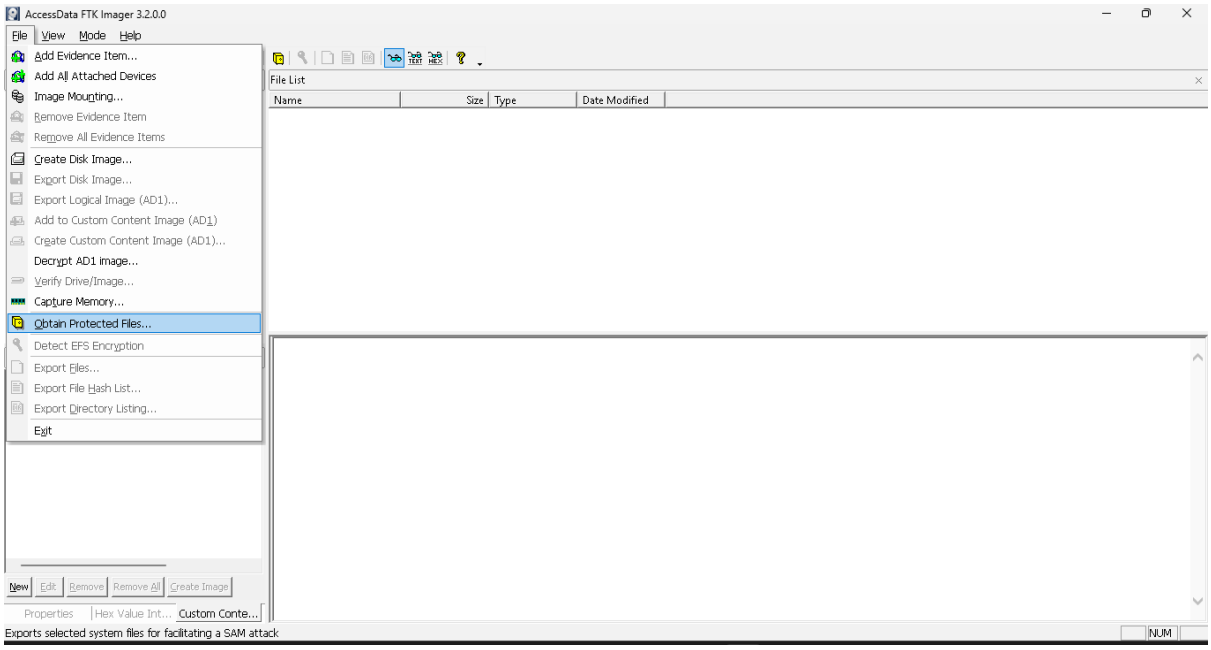


Step 13: Obtaining Protected **Registry Files** Using **FTK Imager**

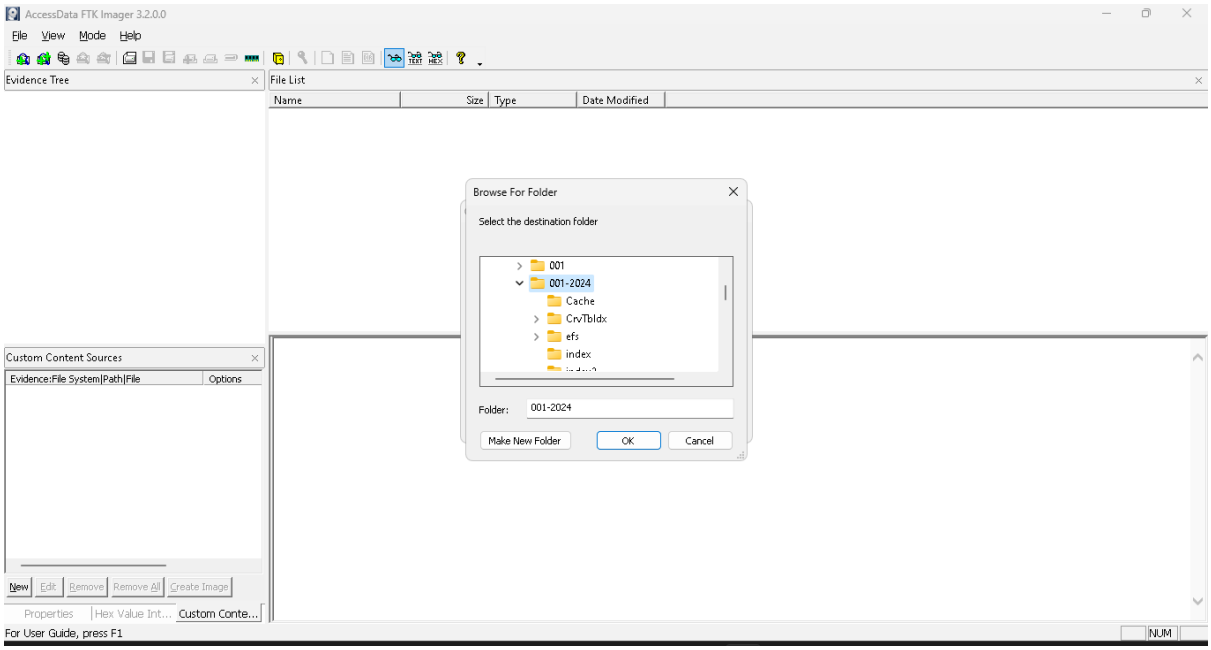
- To obtain the protected **registry files** using **FTK Imager:**
- **Launch FTK Imager.**



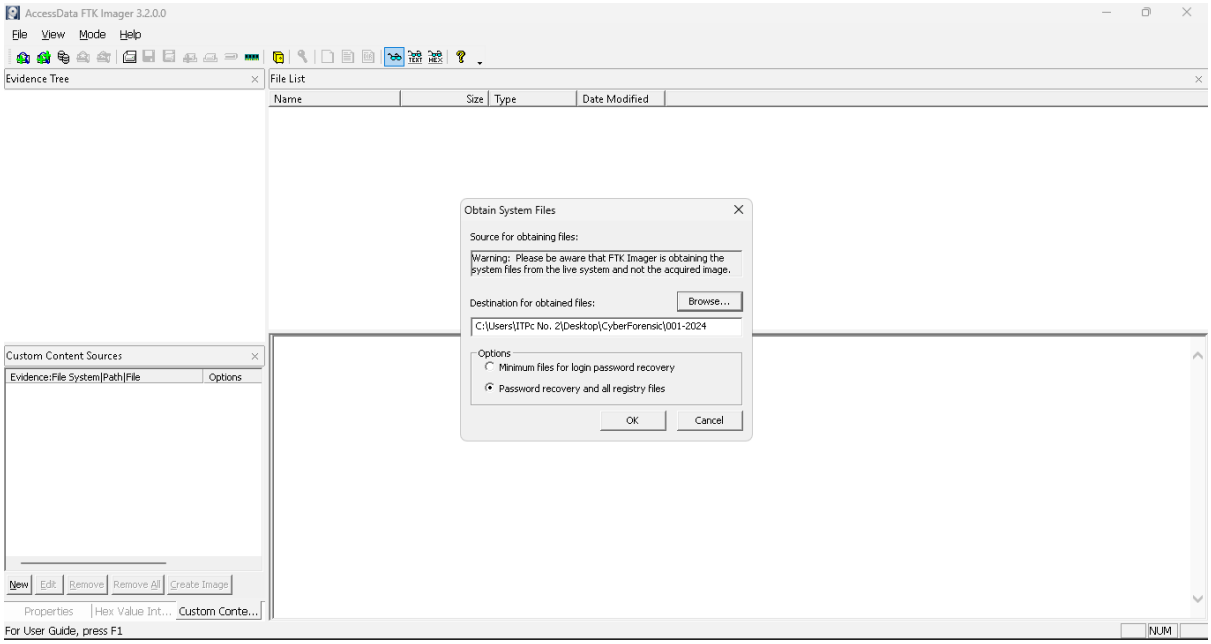
- **Click File,** and then Obtain **Protected Files**



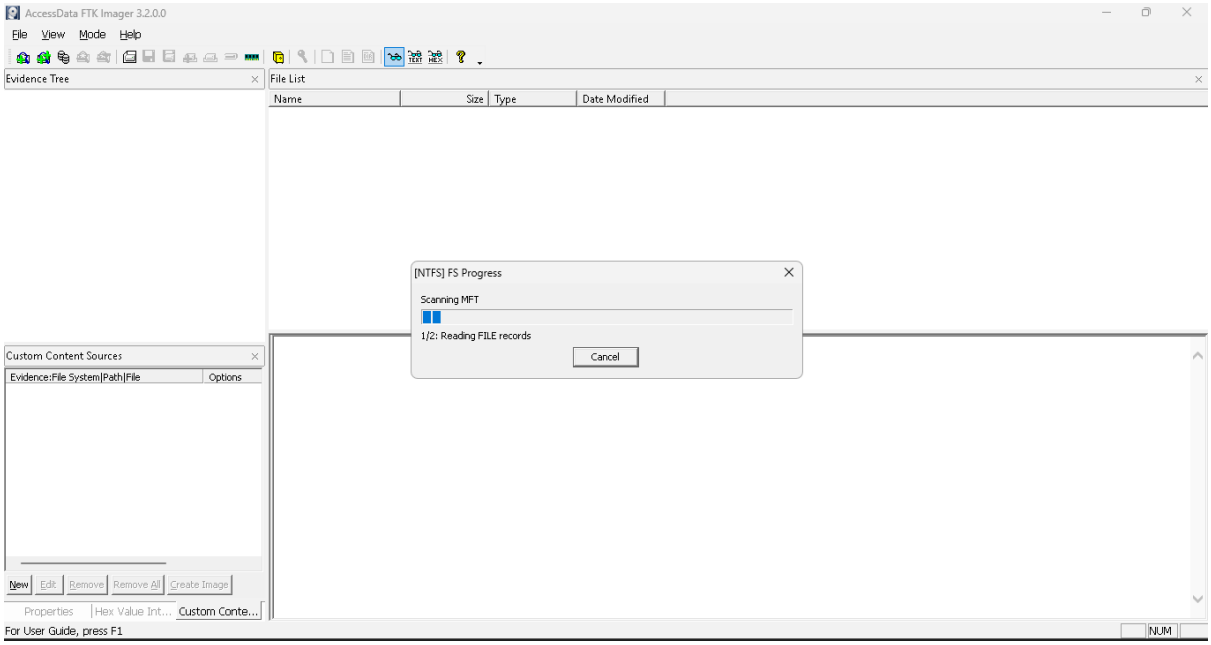
- Select the destination folder **(Here it is 001-2024)** and **Click on OK**



- **Under System Files Options Select Password recovery and all registry files and Click on OK**

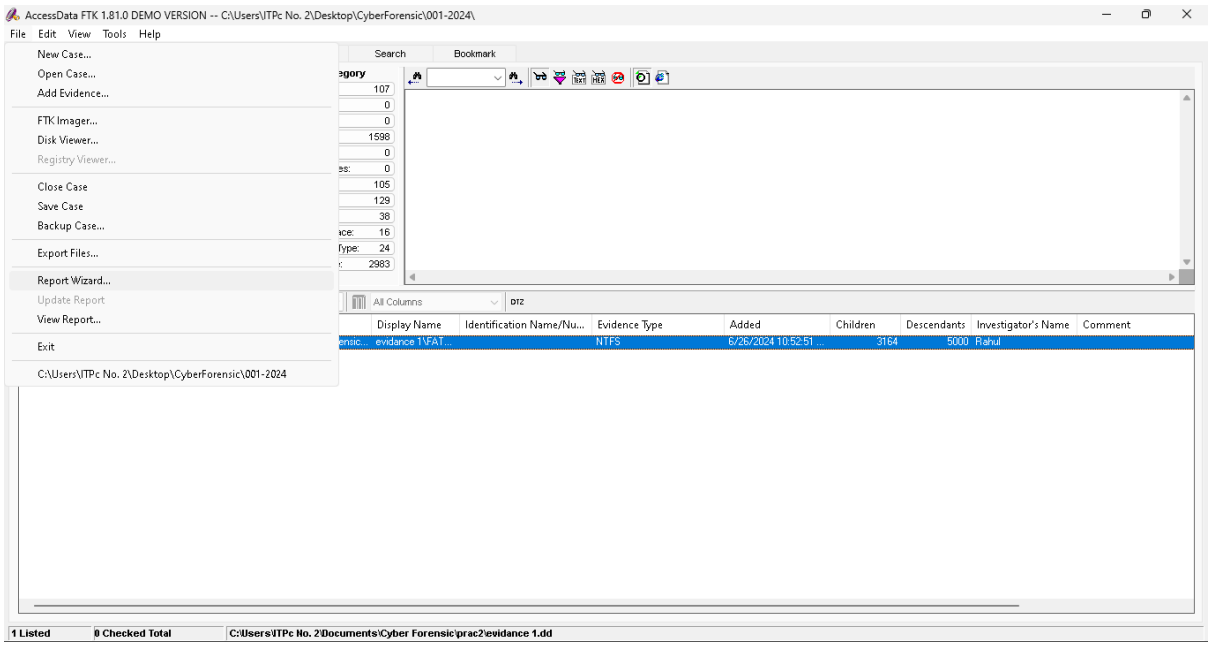


- **Scanning MFT**

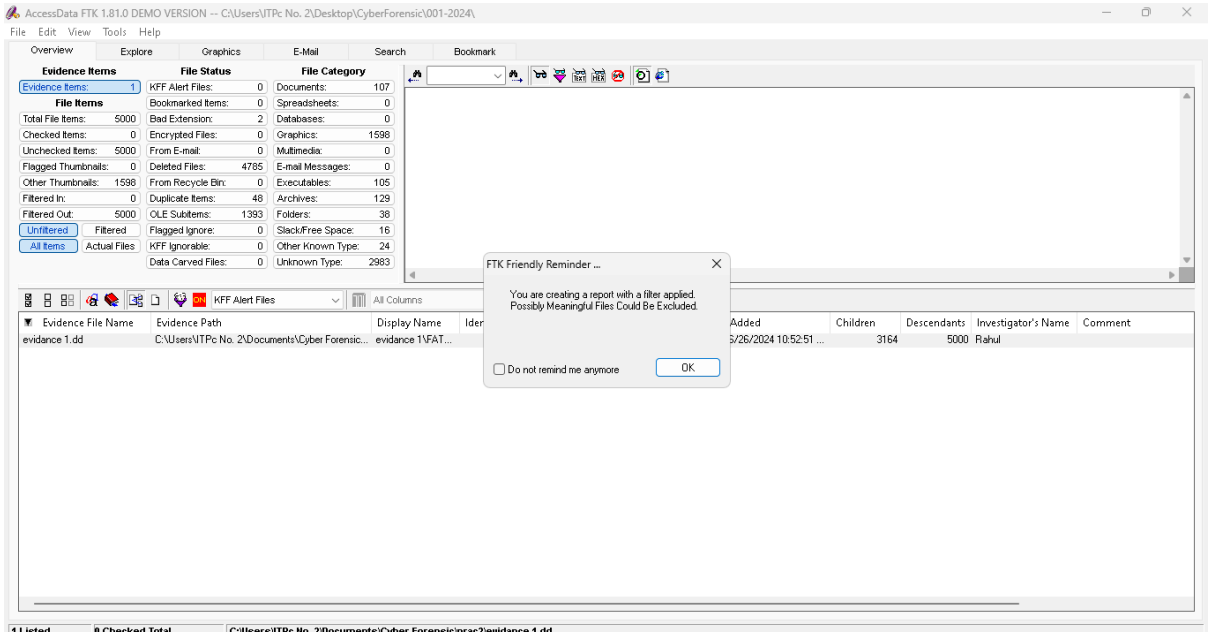


Step 14: Generating a Report

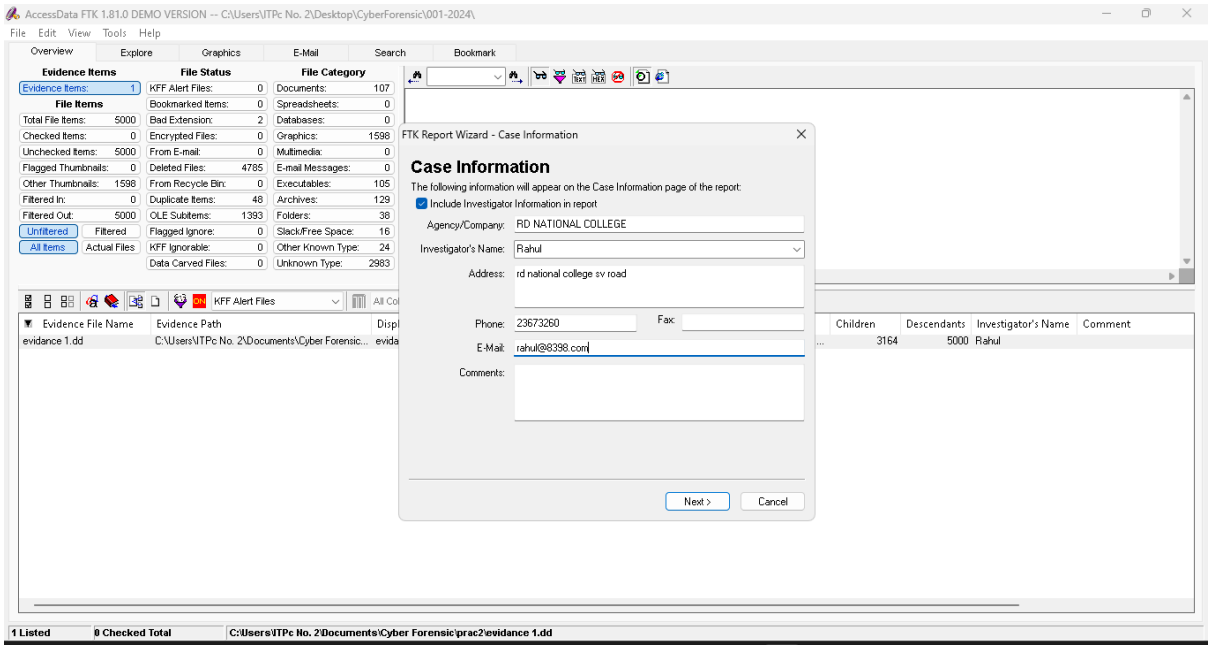
- From the menu, **select Report**, and then **Generate Report** or **click the button on the toolbar**



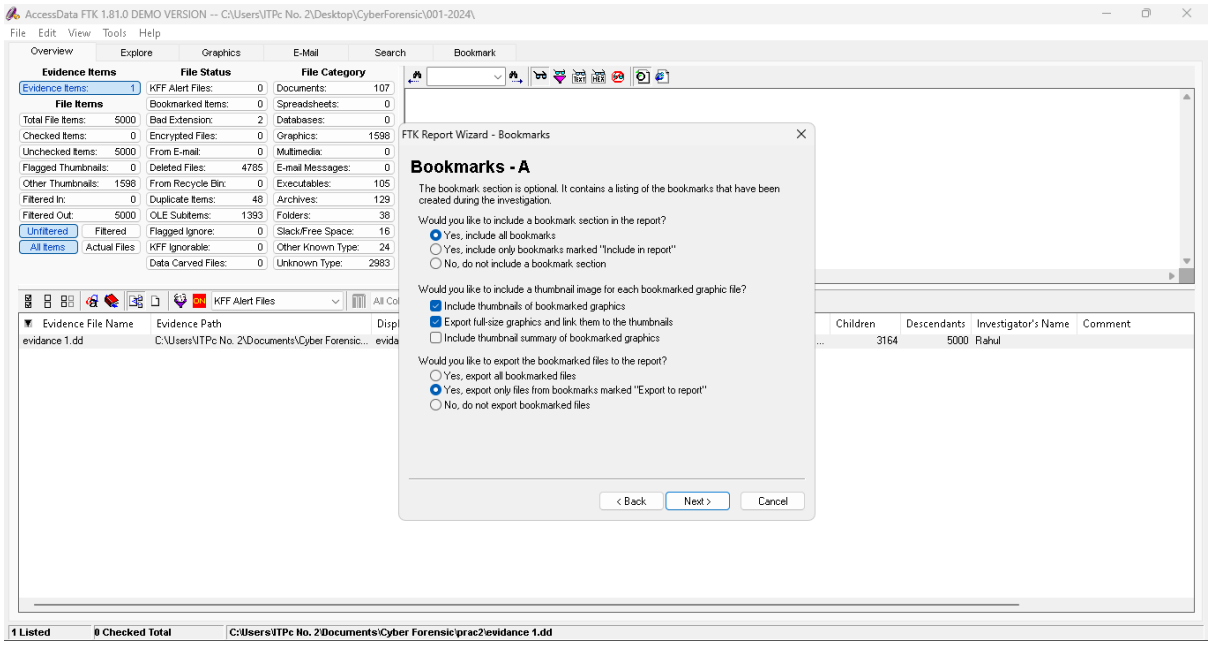
- **Click on OK**



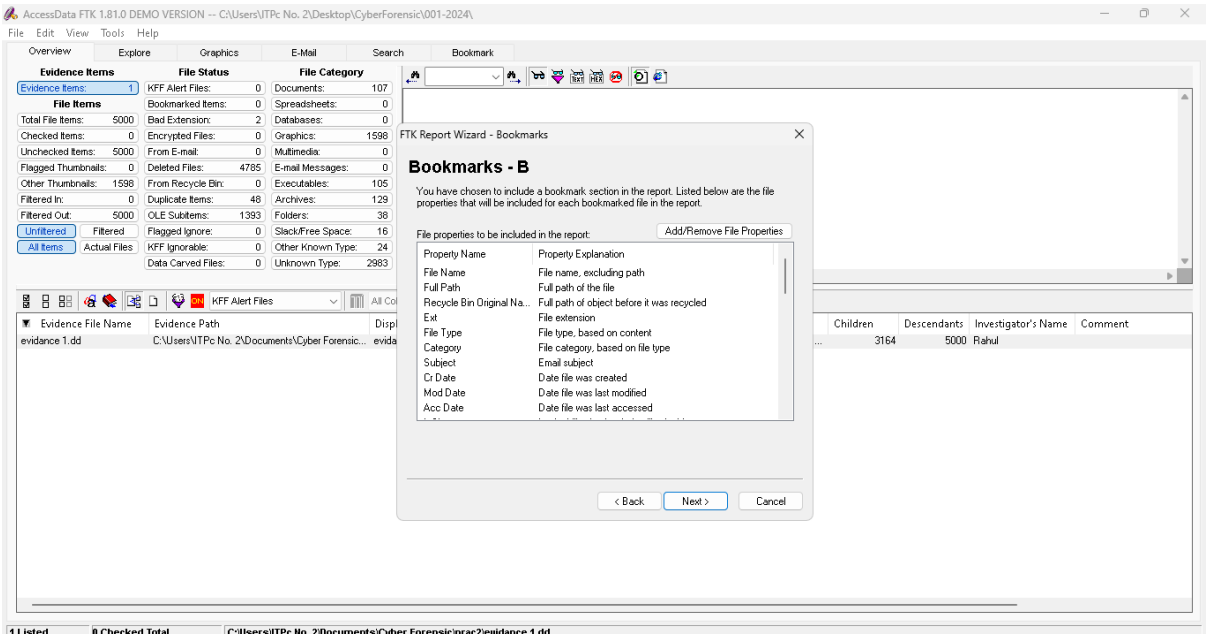
- Under **Case Information** Enter Following Information **and Click on Next**



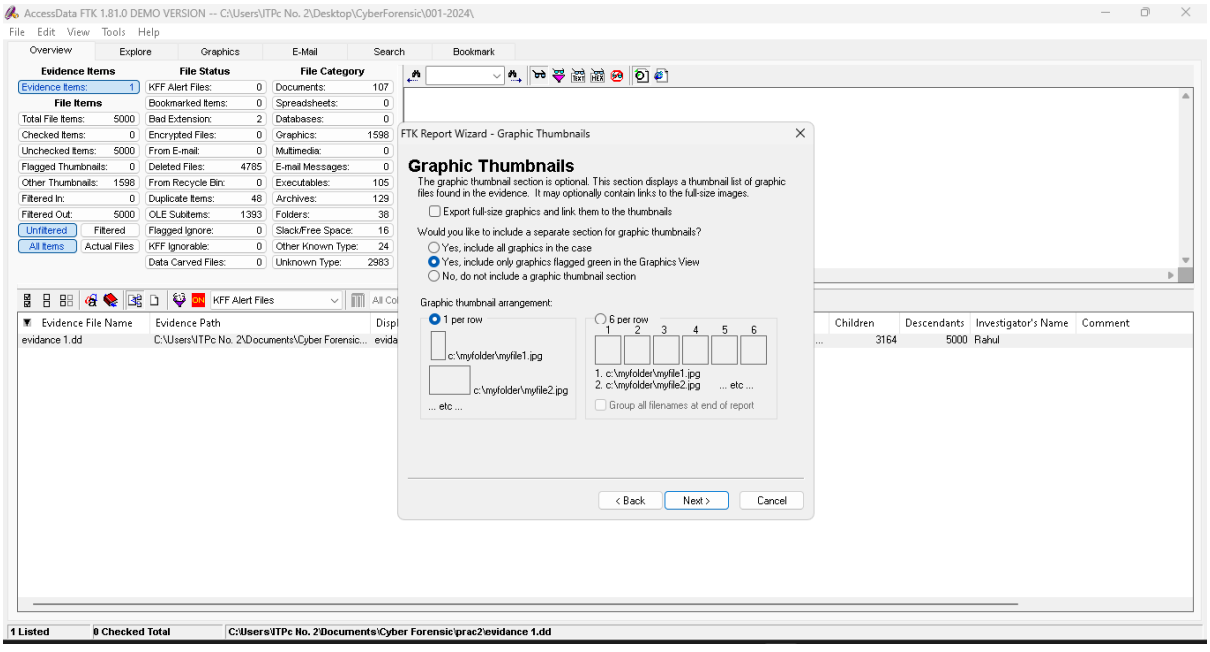
- **Keep the Default Setting** and **Click on Next**



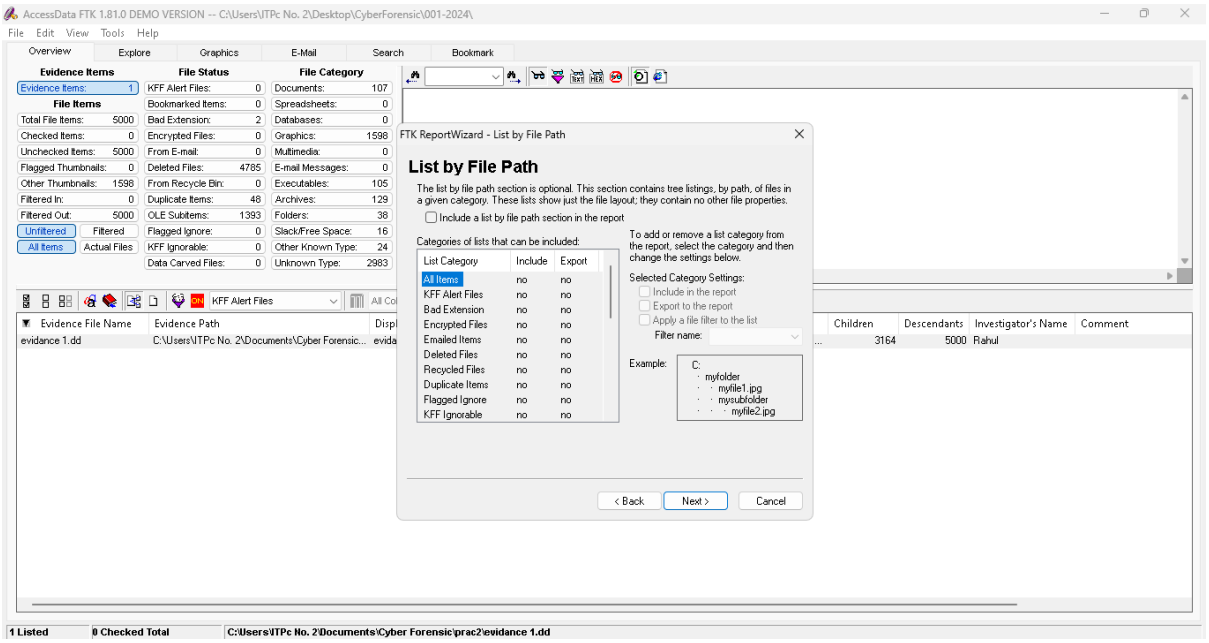
- **Keep the Default Setting** and **Click on Next**



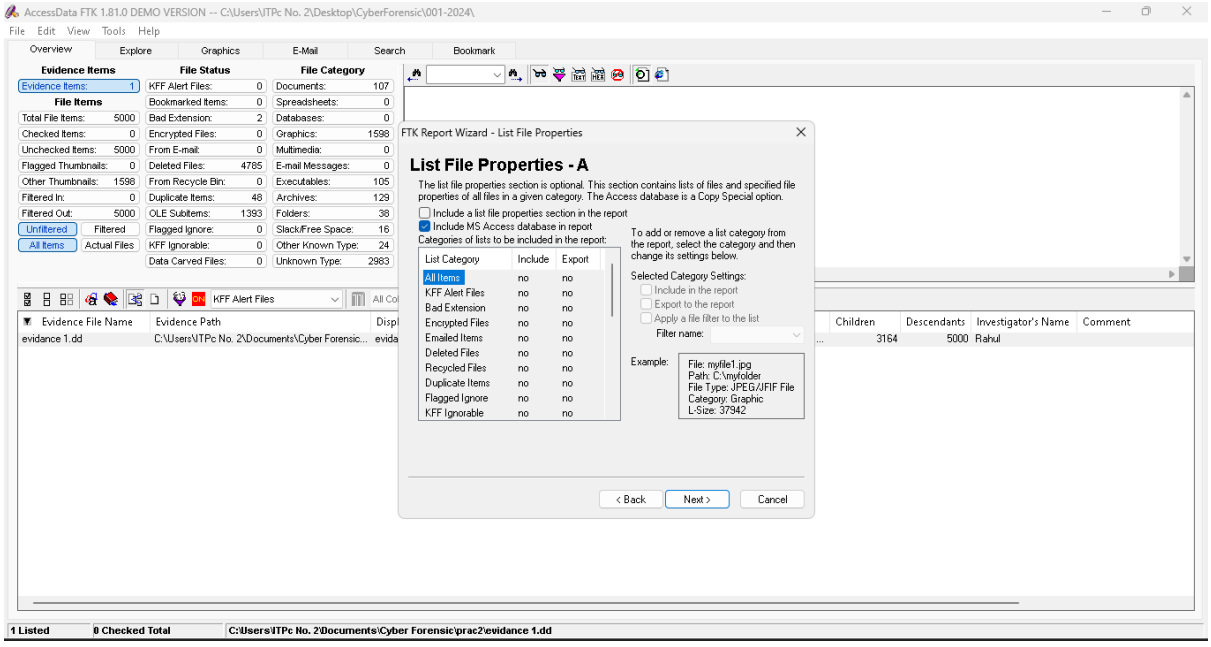
- **Keep the Default Setting** and **Click on Next**



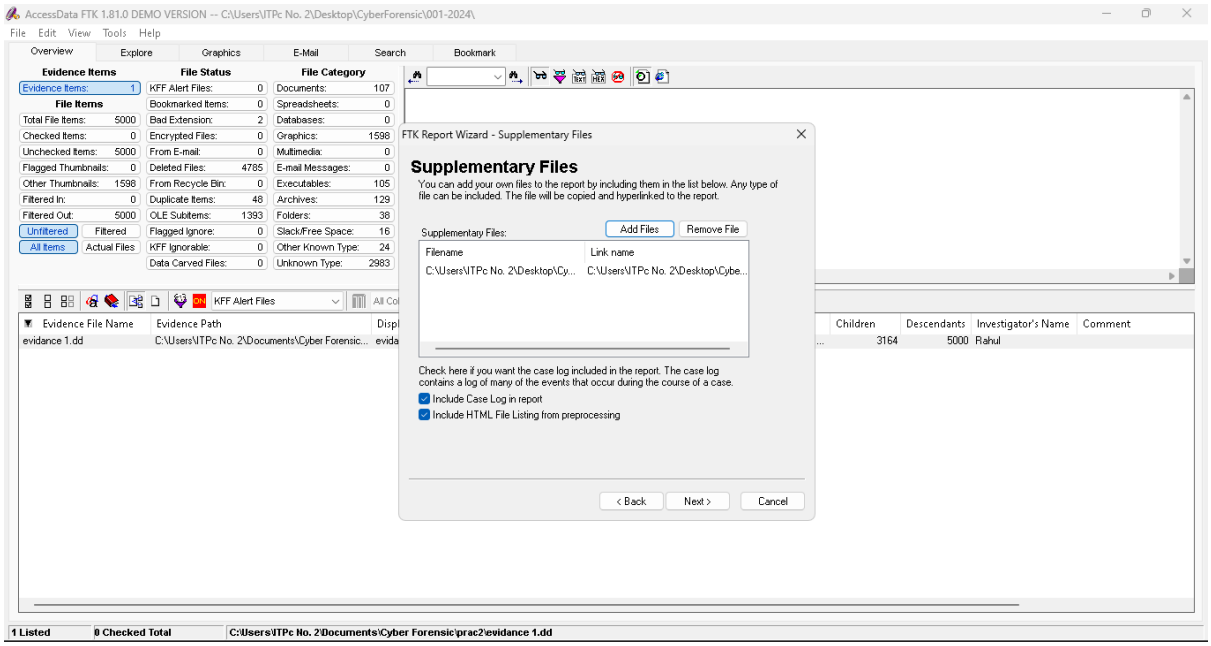
- **Click on Next**



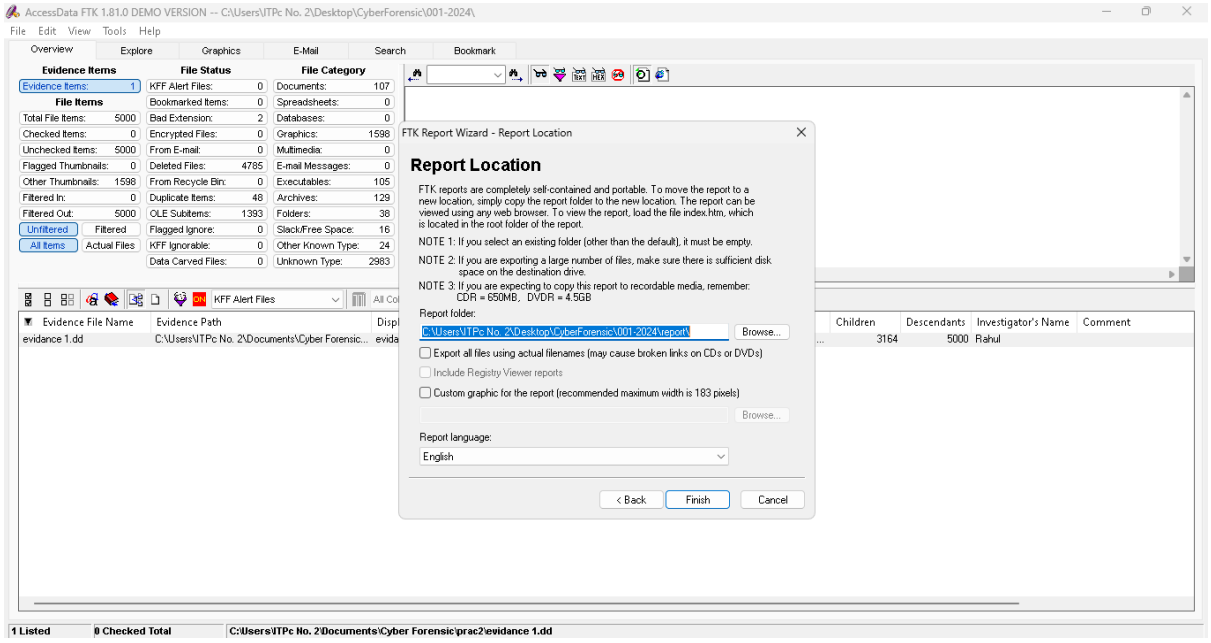
- **Click on Next**



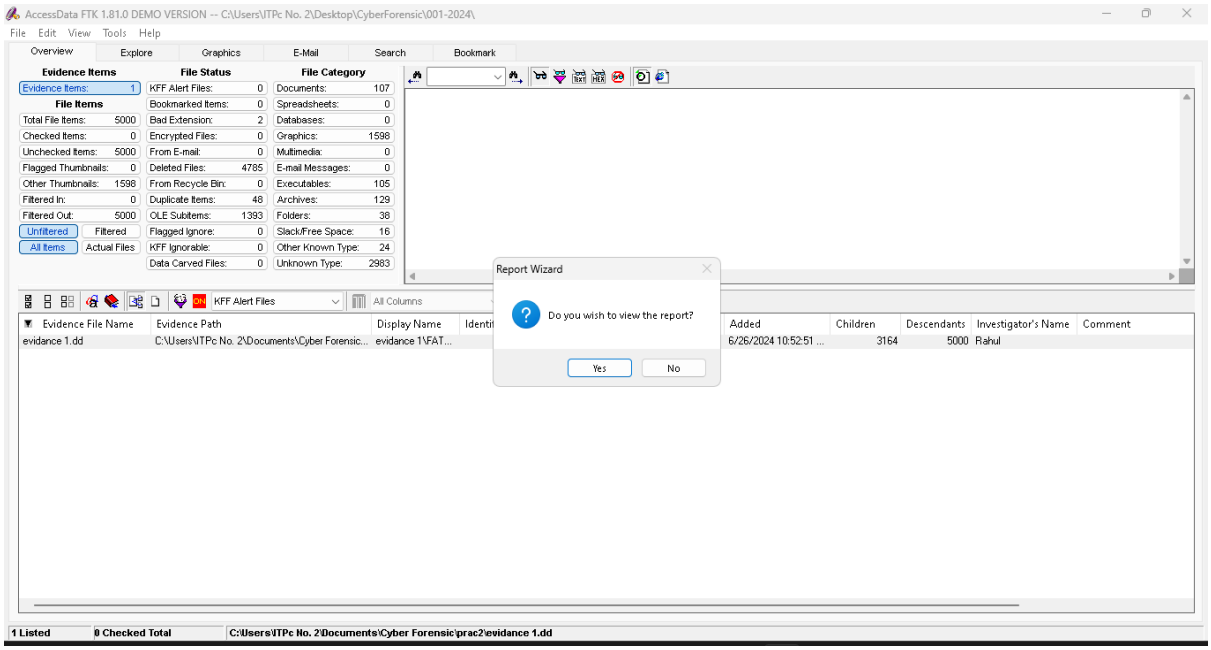
- **Click on Add Files and Select the Supplementary Files and Click on Next**



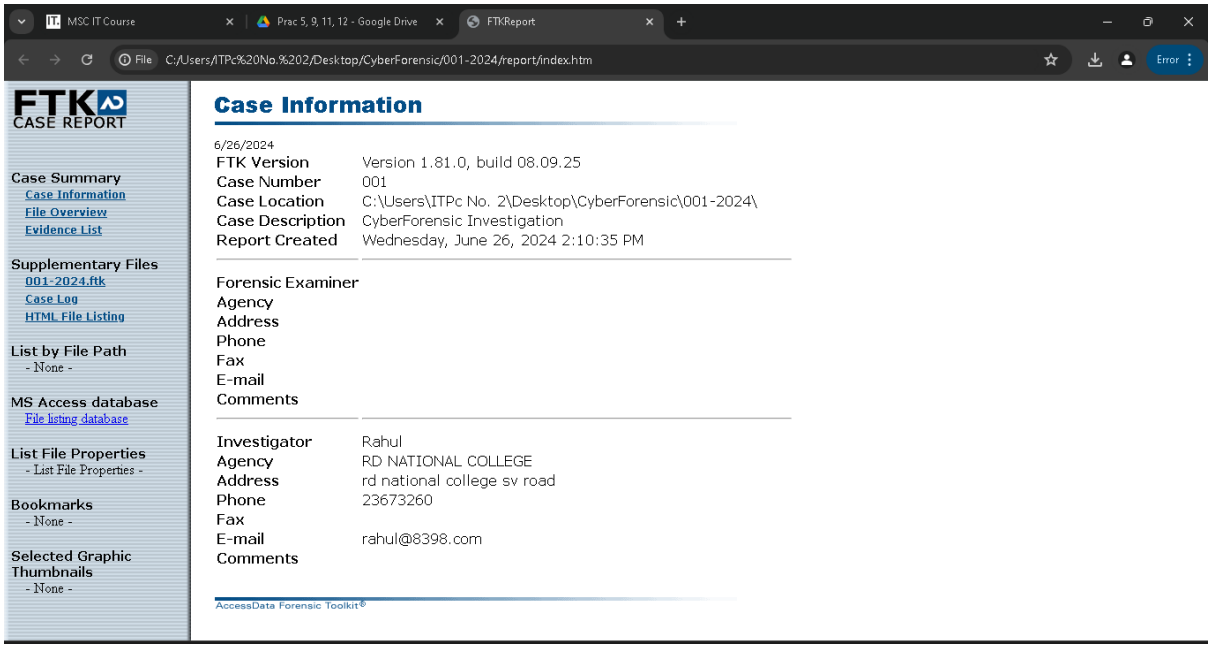
- **Click on Finish**



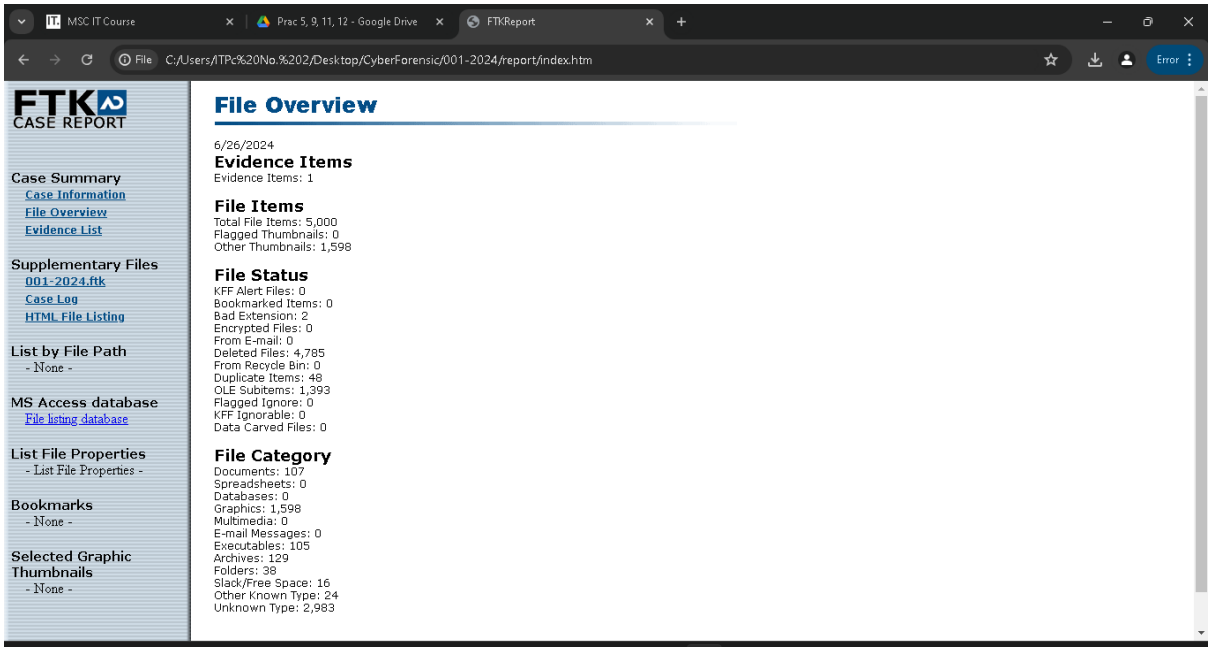
- **Click on OK**

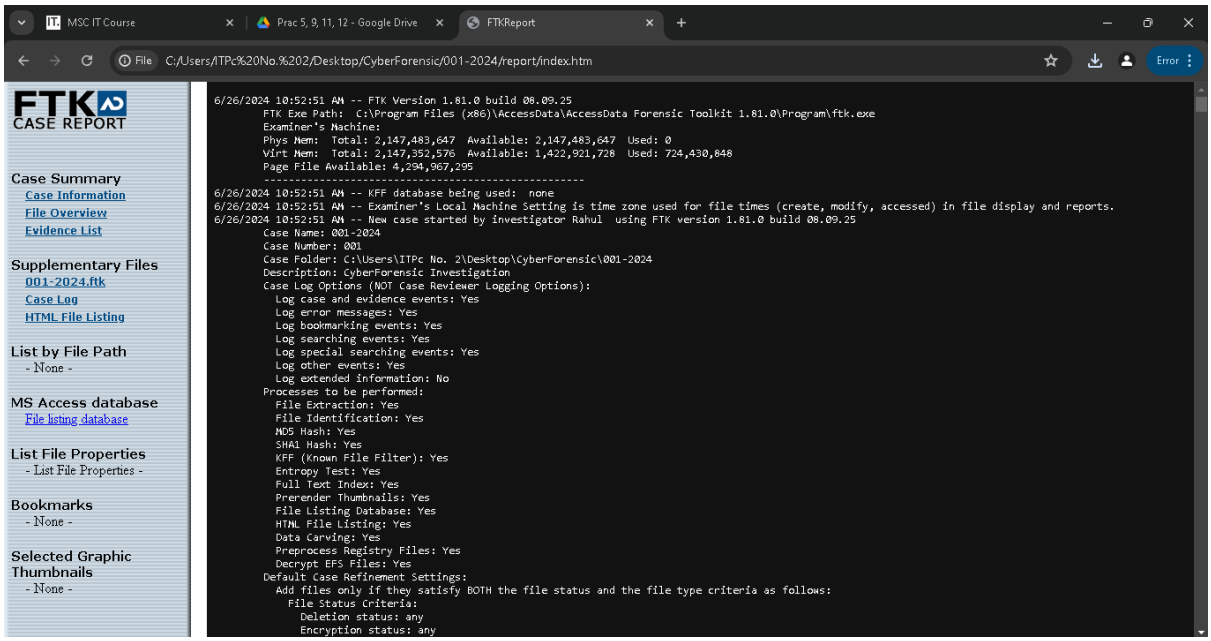


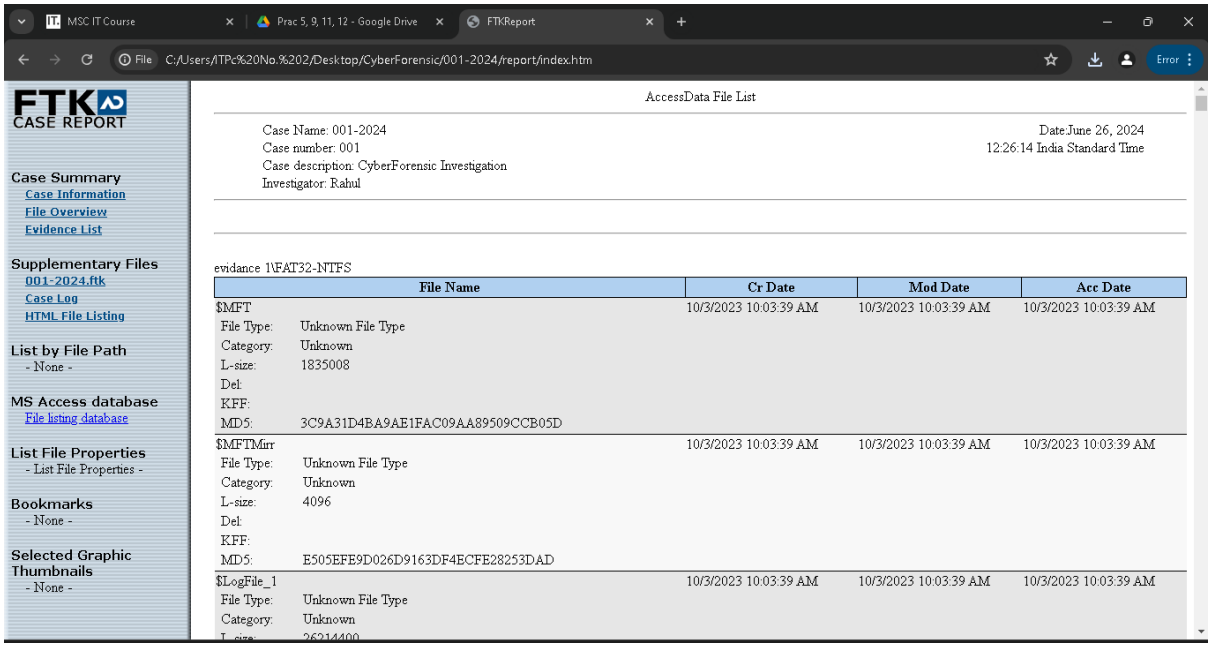
- **Generated Report**



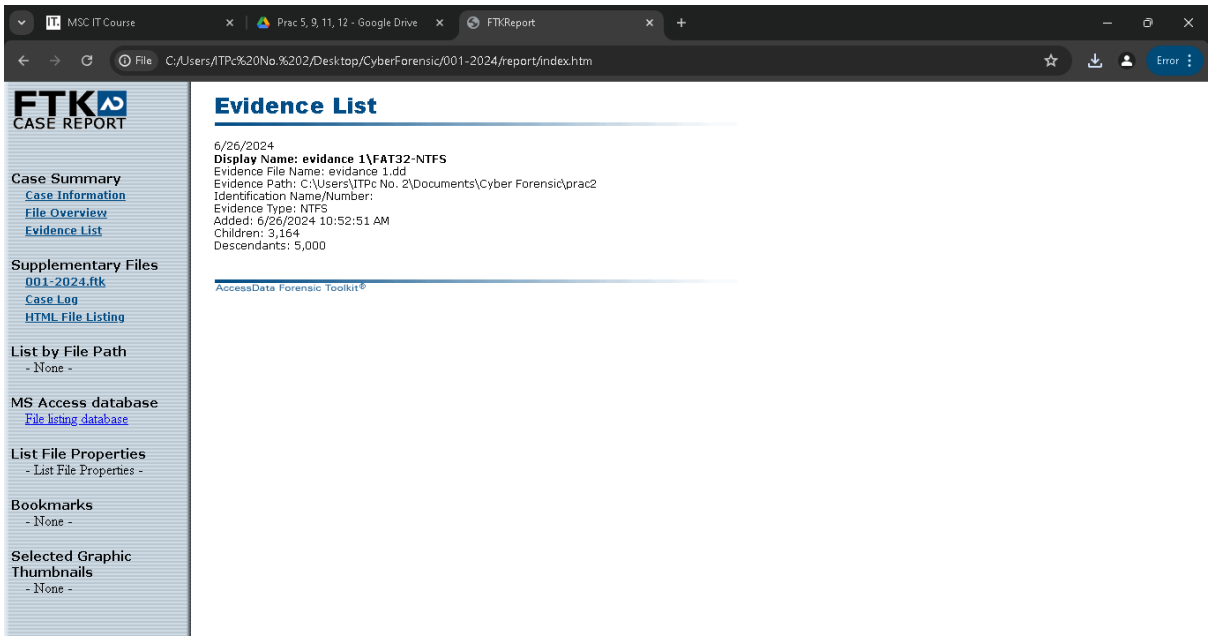
- **File Overview**







- **Evidence List**



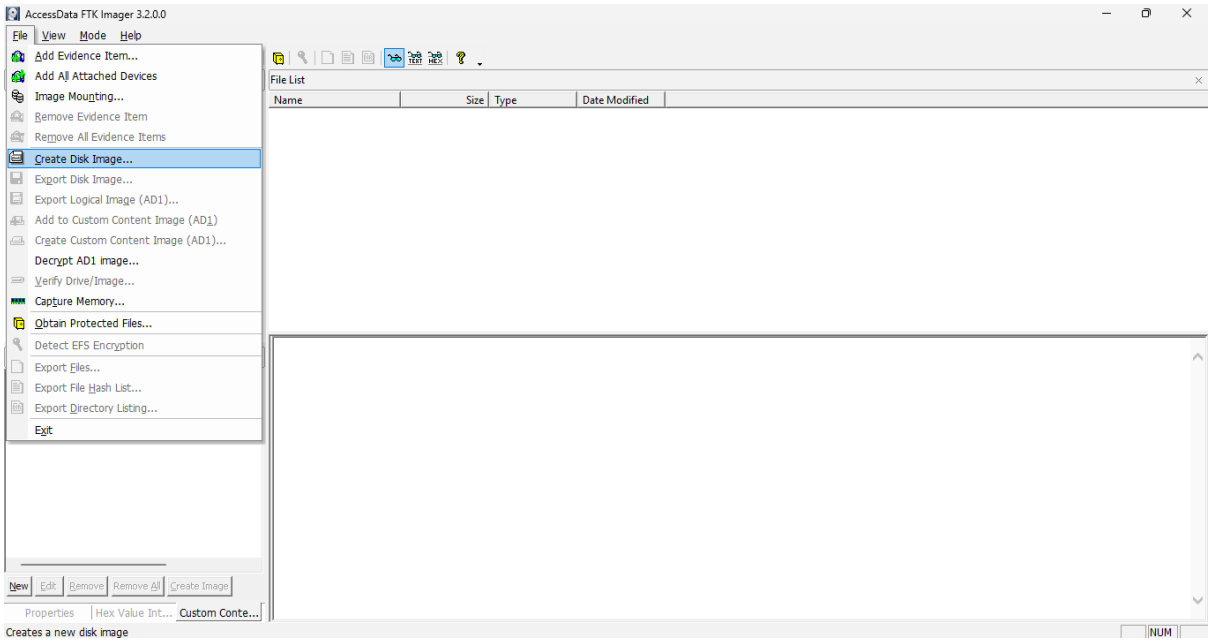
Practical: 3

Aim: Understanding & working with the process of taking a drive image using AccessData's FTK Imager tool.

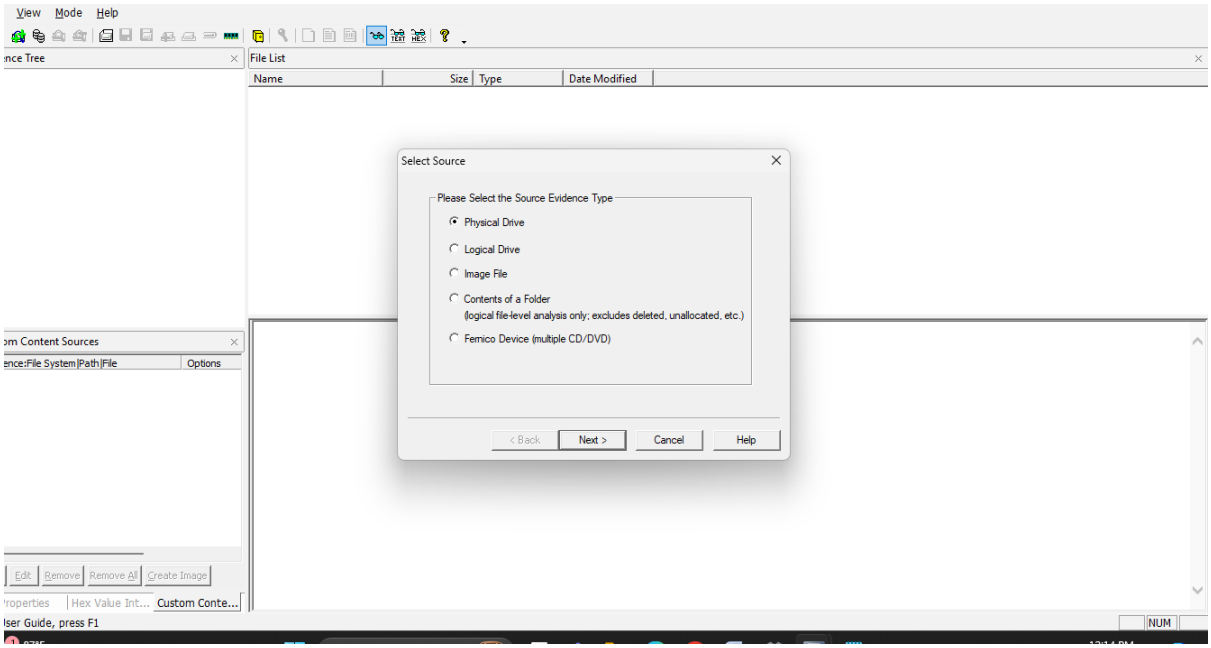
Writeup:

Step 1: Run **FTK Imager.exe** to start the tool

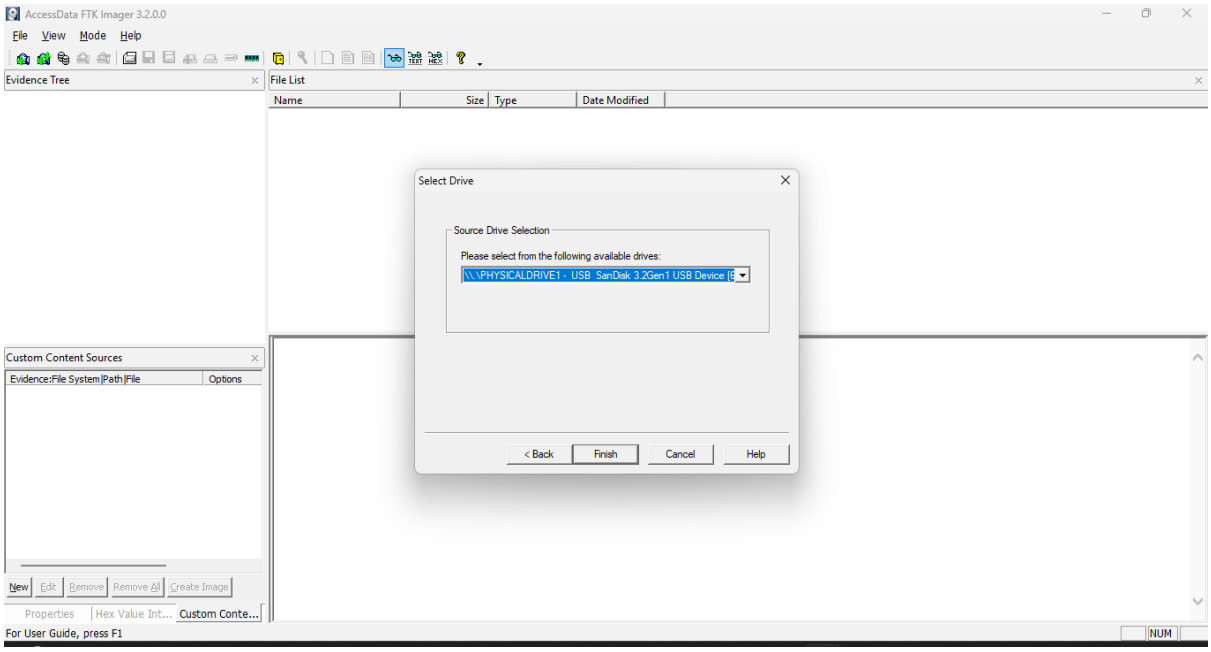
- **Click on File** and **Select Create Disk image**



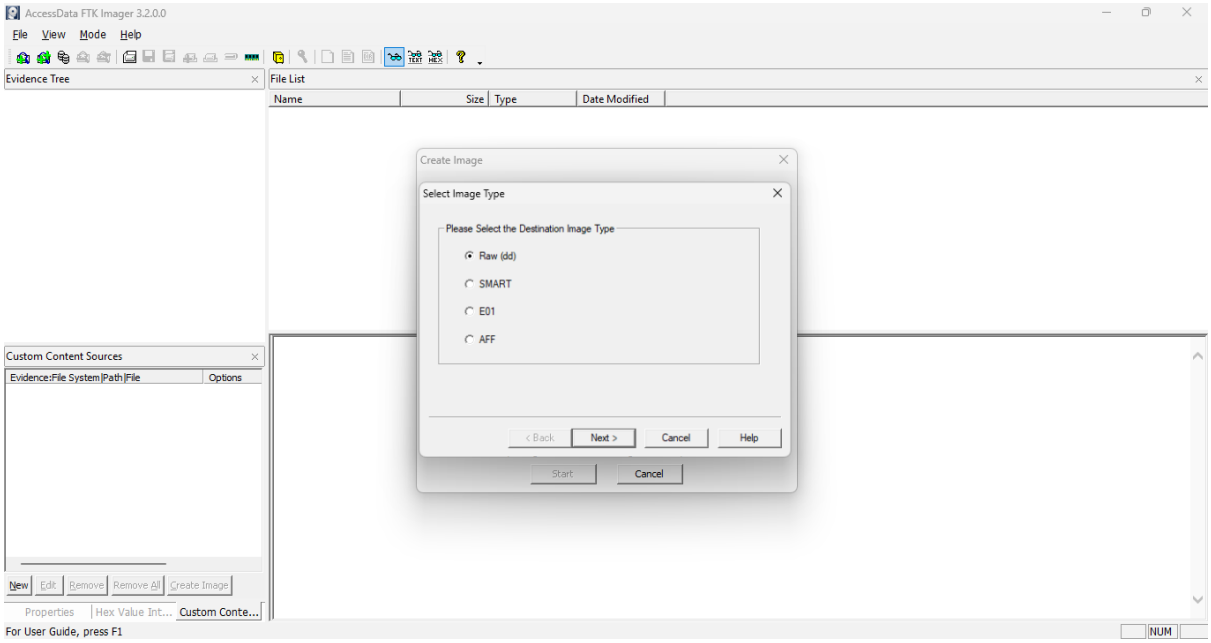
Step 2: In the Select Source dialog box, select the source you want to make an image of (Here it is **Physical Drive). Click Next.**



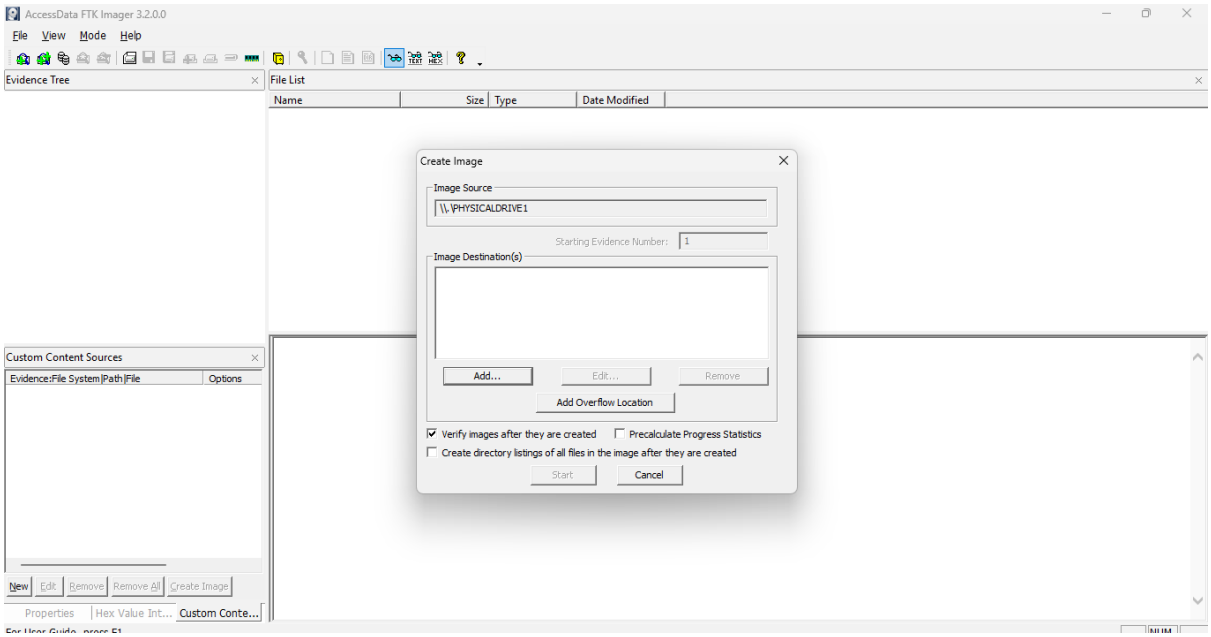
Step 3: Select the drive or browse to the source of the image you want, and then **click Finish.**



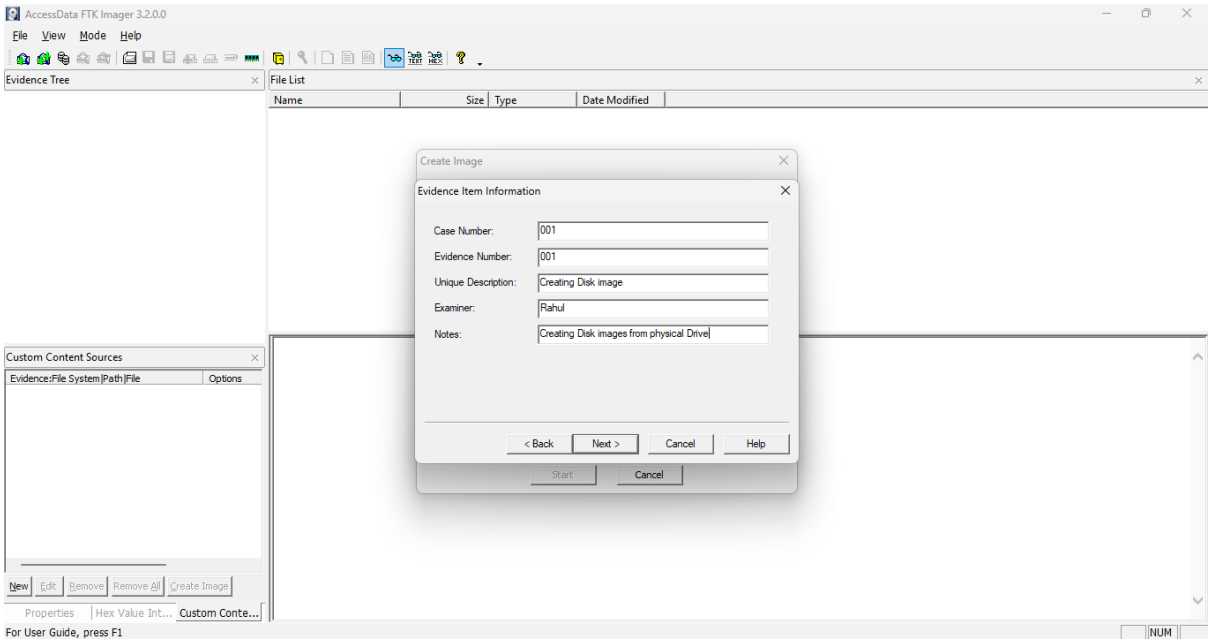
Step 4: Within **Select Image Type Select Raw (dd)** and **Click on Next**



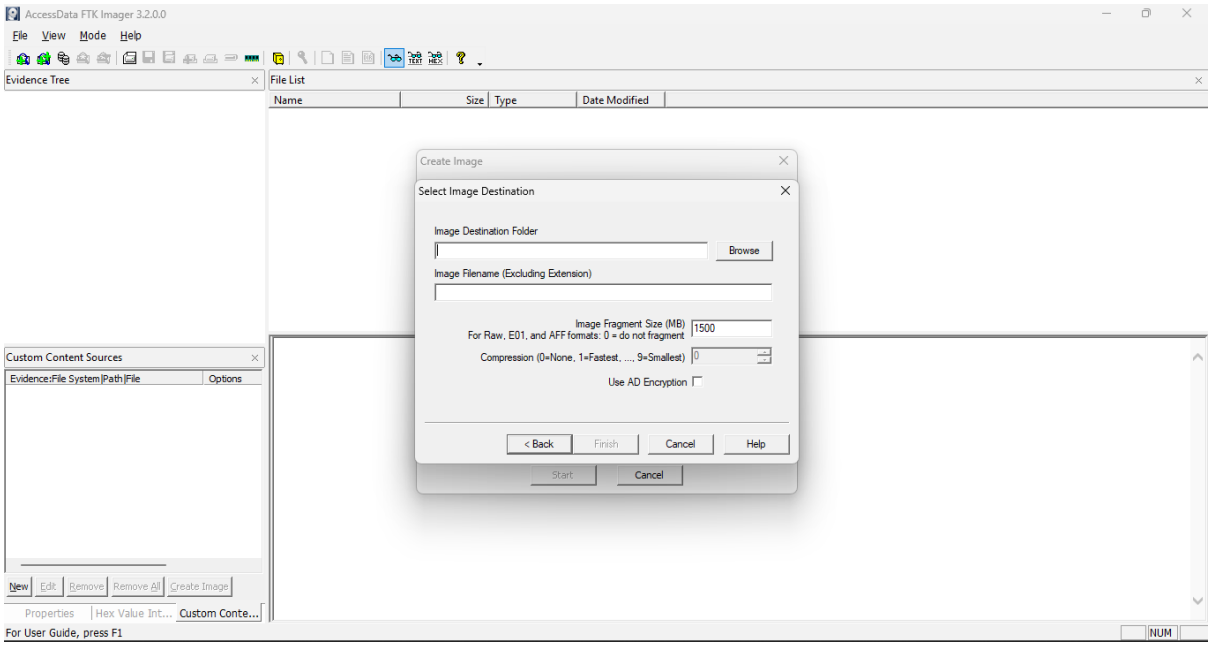
Step 5: Within **Image Destination Click on Add**



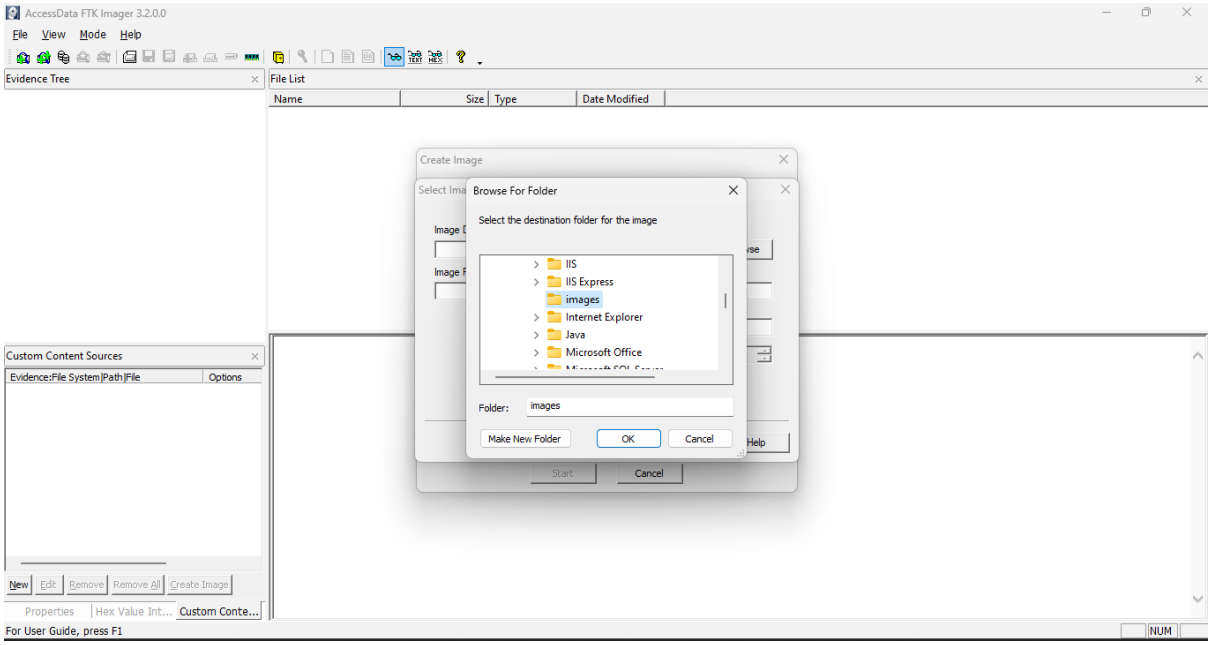
- Under **Evidence Item Information** Enter the Following Information and **Click on Next**



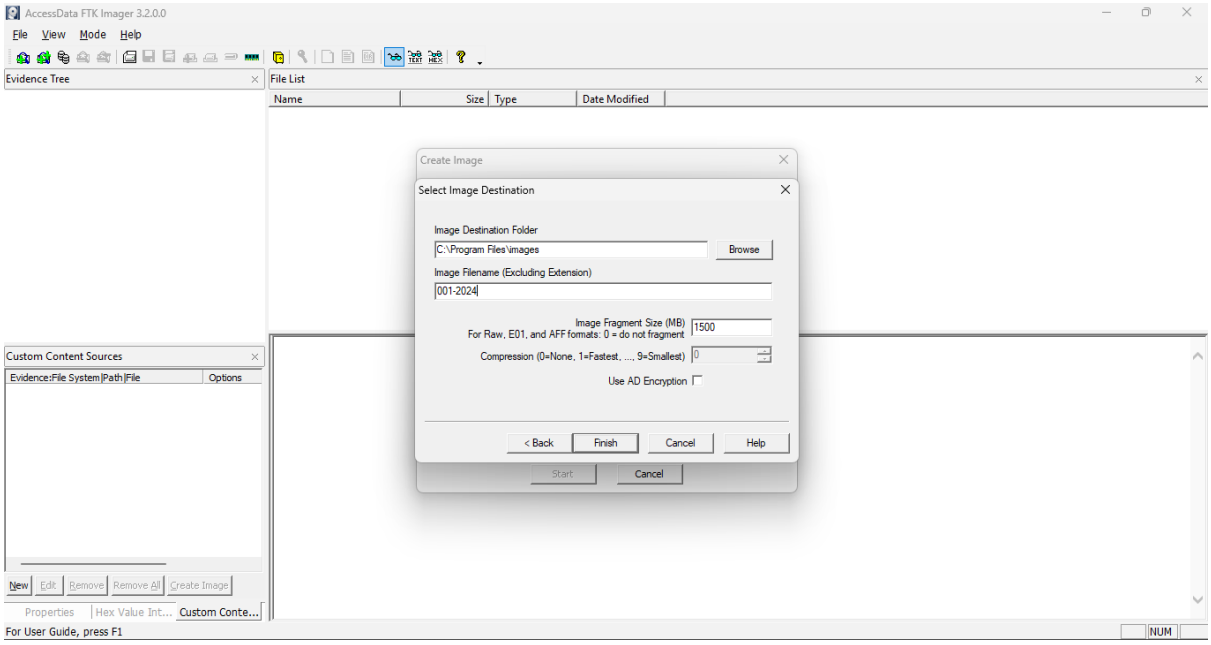
- Within Image Destination Folder **Click on Browse**



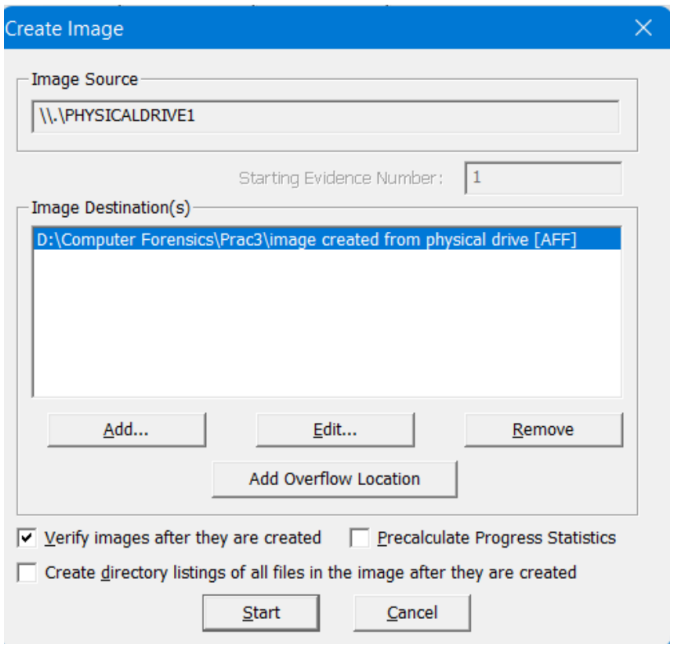
- Within **Select the destination folder for the image Select images folder** and **click on OK**



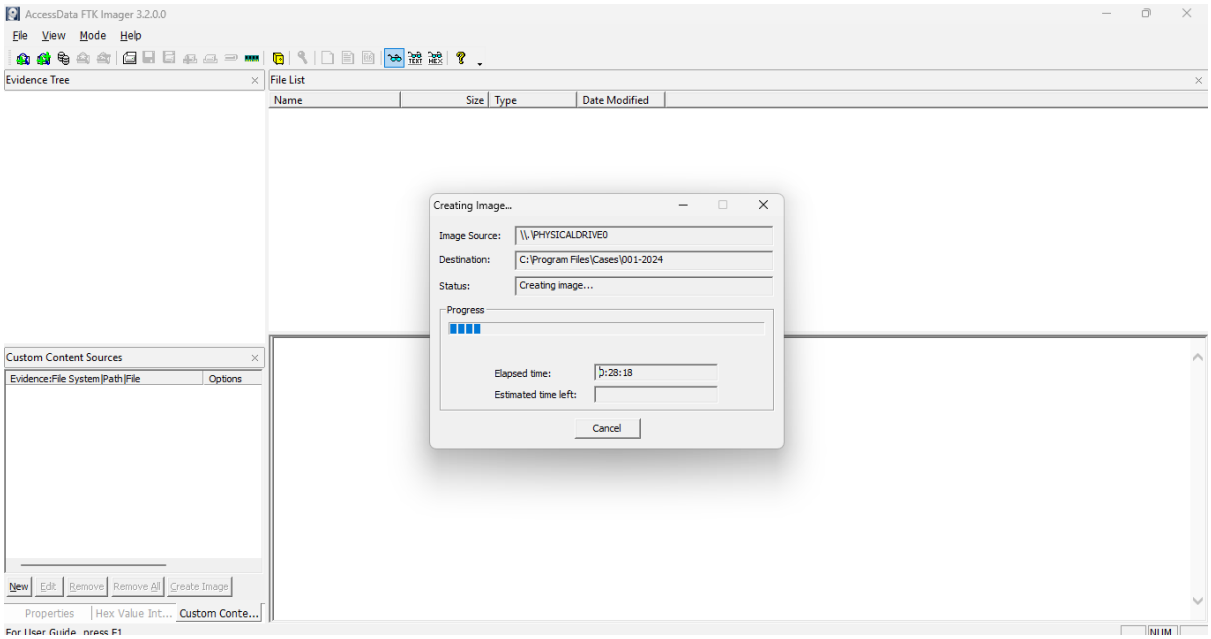
- Type **Image Filename Here it is 001-2024** and **Click on Finish**



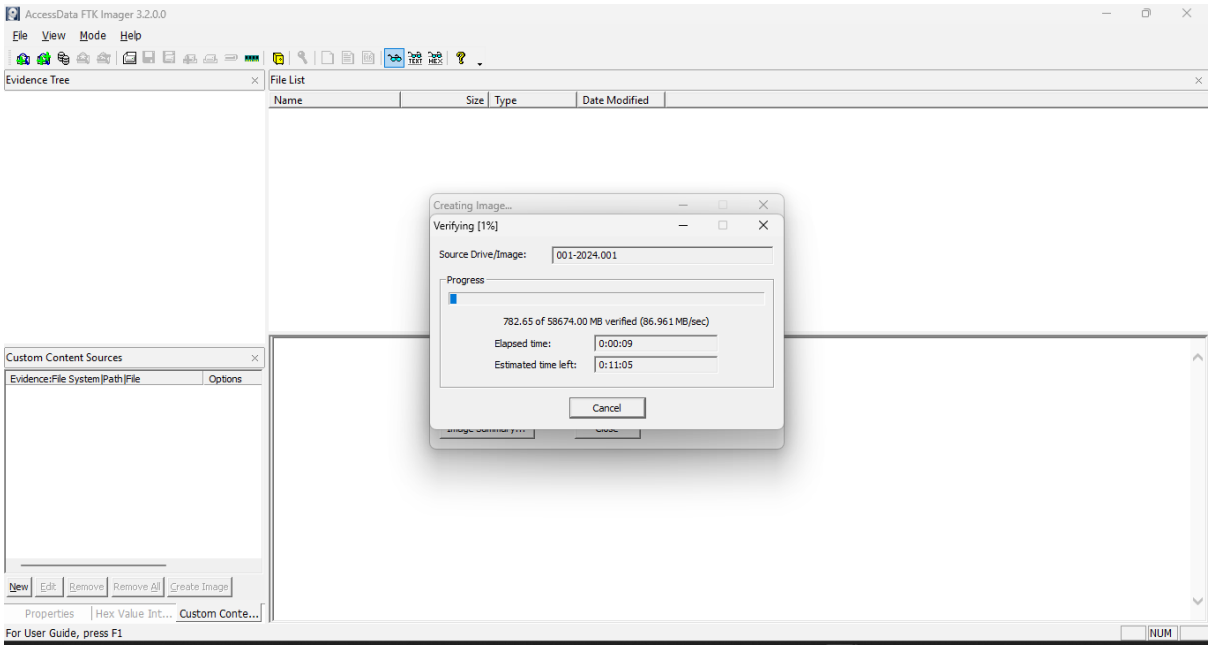
- **Click Start** to begin the imaging process.



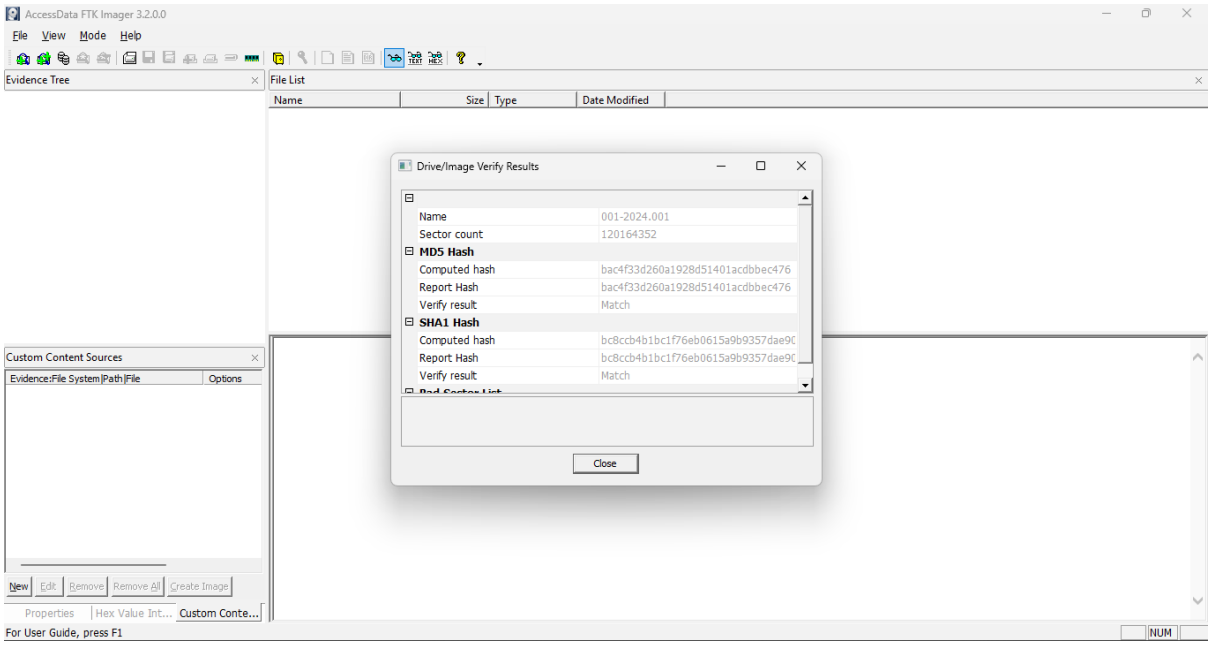
- Image Creation Process Start



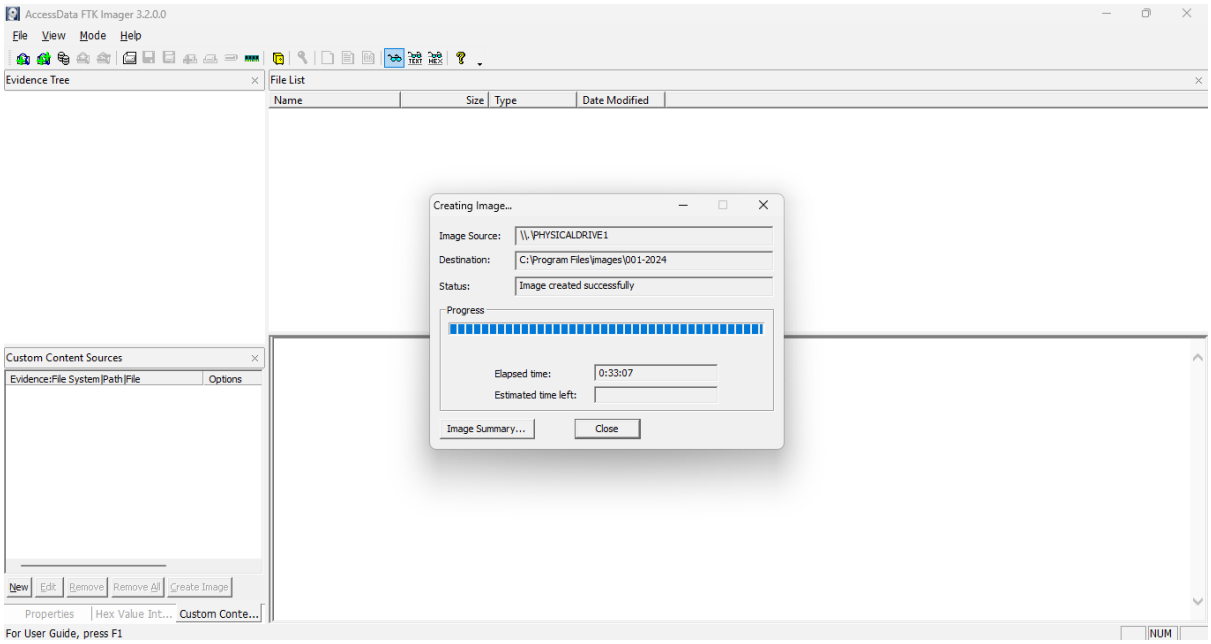
- After the images are successfully created, the Drive/Image Verify Results box shows detailed image information, including MD5 and SHA1 check sums, and bad sectors



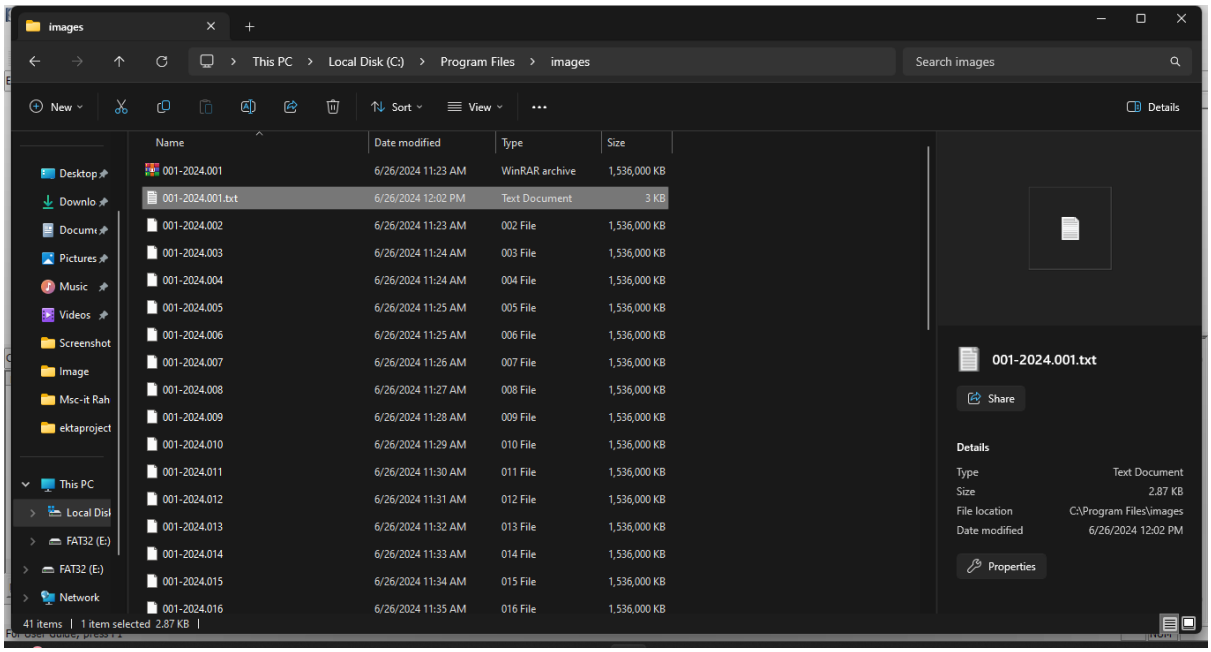
- Once the acquisition is complete, you can view an image summary and the drive will appear in the evidence list in the left hand side of the main FTK Imager window. You can right-click on the drive name to Verify the Image

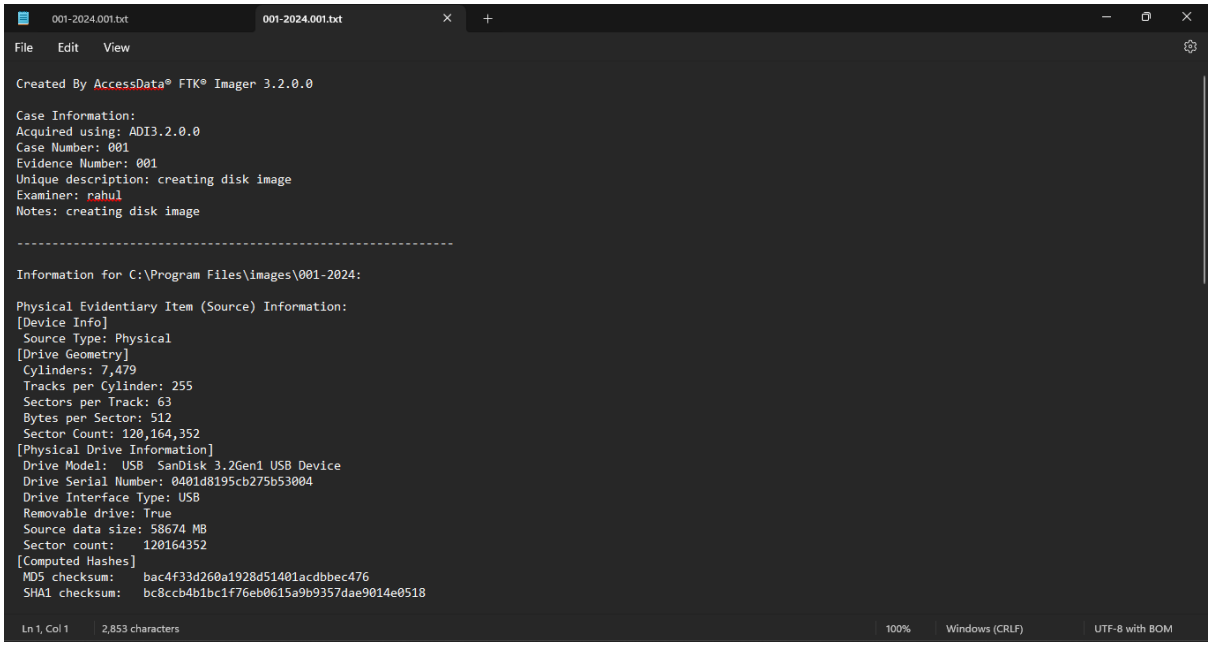


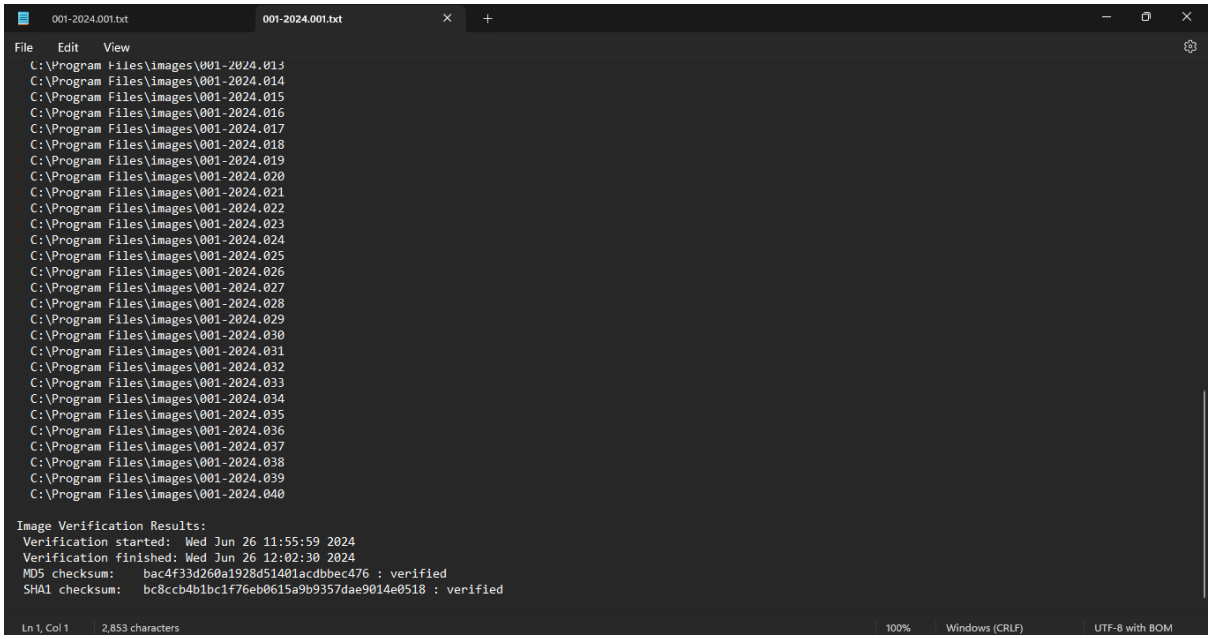
- **Image Created Successfully**



Step 6: After Creation of Image of One text document created (Here it is 001-2024.txt). it give image information






001-2024.001.txt
001-2024.001.txt
File Edit View
C:\Program Files\images\001-2024.013
C:\Program Files\images\001-2024.014
C:\Program Files\images\001-2024.015
C:\Program Files\images\001-2024.016
C:\Program Files\images\001-2024.017
C:\Program Files\images\001-2024.018
C:\Program Files\images\001-2024.019
C:\Program Files\images\001-2024.020
C:\Program Files\images\001-2024.021
C:\Program Files\images\001-2024.022
C:\Program Files\images\001-2024.023
C:\Program Files\images\001-2024.024
C:\Program Files\images\001-2024.025
C:\Program Files\images\001-2024.026
C:\Program Files\images\001-2024.027
C:\Program Files\images\001-2024.028
C:\Program Files\images\001-2024.029
C:\Program Files\images\001-2024.030
C:\Program Files\images\001-2024.031
C:\Program Files\images\001-2024.032
C:\Program Files\images\001-2024.033
C:\Program Files\images\001-2024.034
C:\Program Files\images\001-2024.035
C:\Program Files\images\001-2024.036
C:\Program Files\images\001-2024.037
C:\Program Files\images\001-2024.038
C:\Program Files\images\001-2024.039
C:\Program Files\images\001-2024.040
Image Verification Results:
Verification started: Wed Jun 26 11:55:59 2024
Verification finished: Wed Jun 26 12:02:30 2024
MD5 checksum: bac4f33d260a1928d51401acdbbec476 : verified
SHA1 checksum: bc8ccb4b1bc1f76eb0615a9b9357dae9014e0518 : verified
Ln 1, Col 1
2,853 characters
100%
Windows (CRLF)
UTF-8 with BOM

Practical: 4

Aim: Using Wireshark Tool.

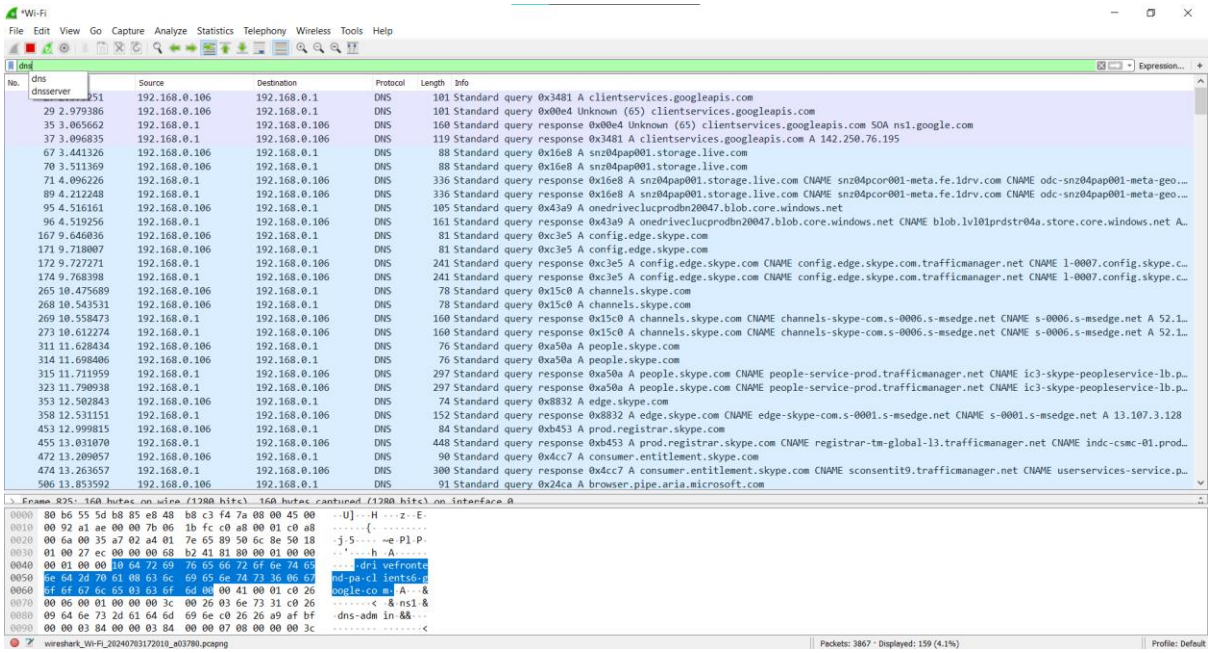
Writeup:

Wireshark is a network packet analyzer that intercepts, captures and logs information about packets passing through a network interface. This is useful for analyzing network problems, detecting network intrusions, network misuse, and other security problems, monitor usage and gather statistics, and many other applications.

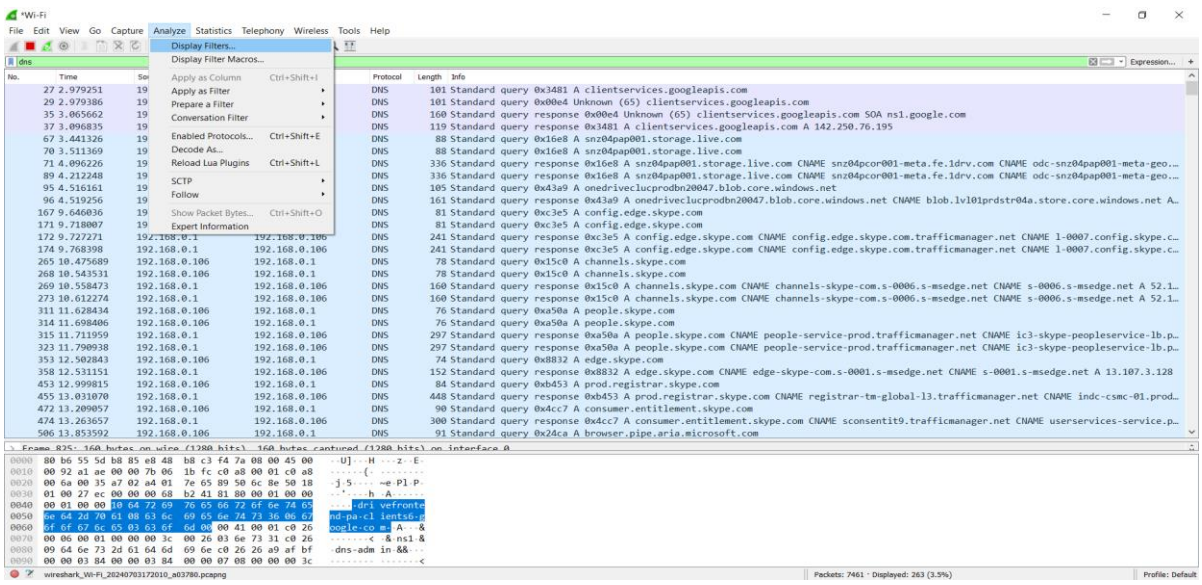
Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount, of packets to sift through. That's where Wireshark's filters come in.

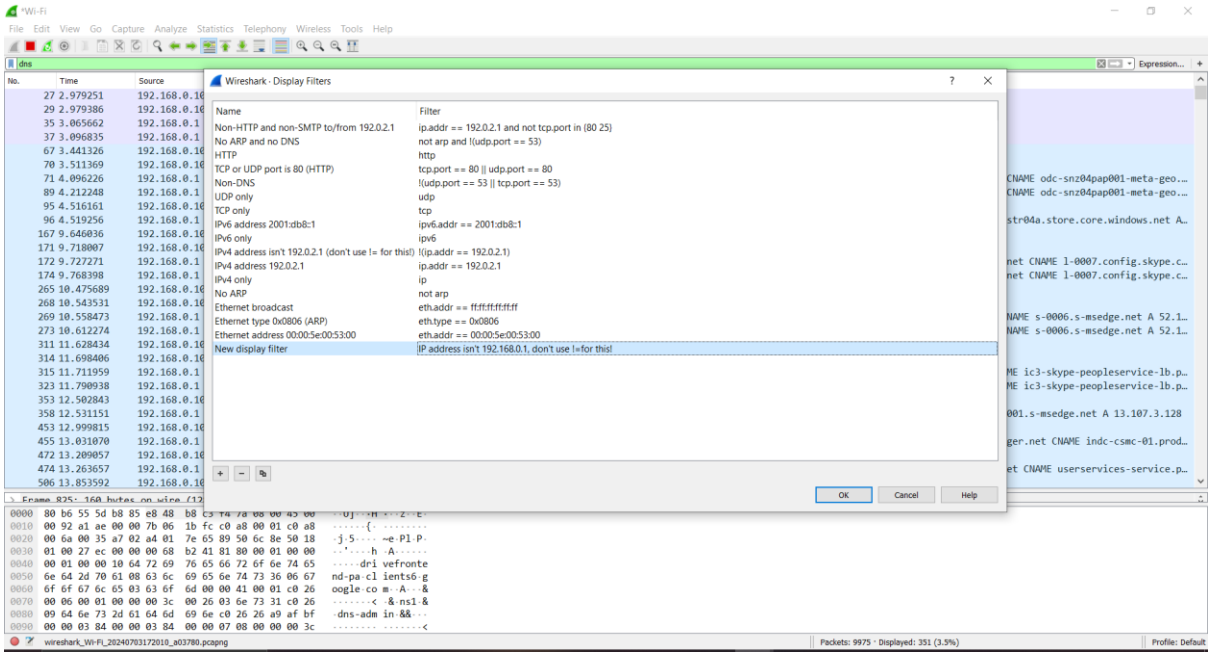
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



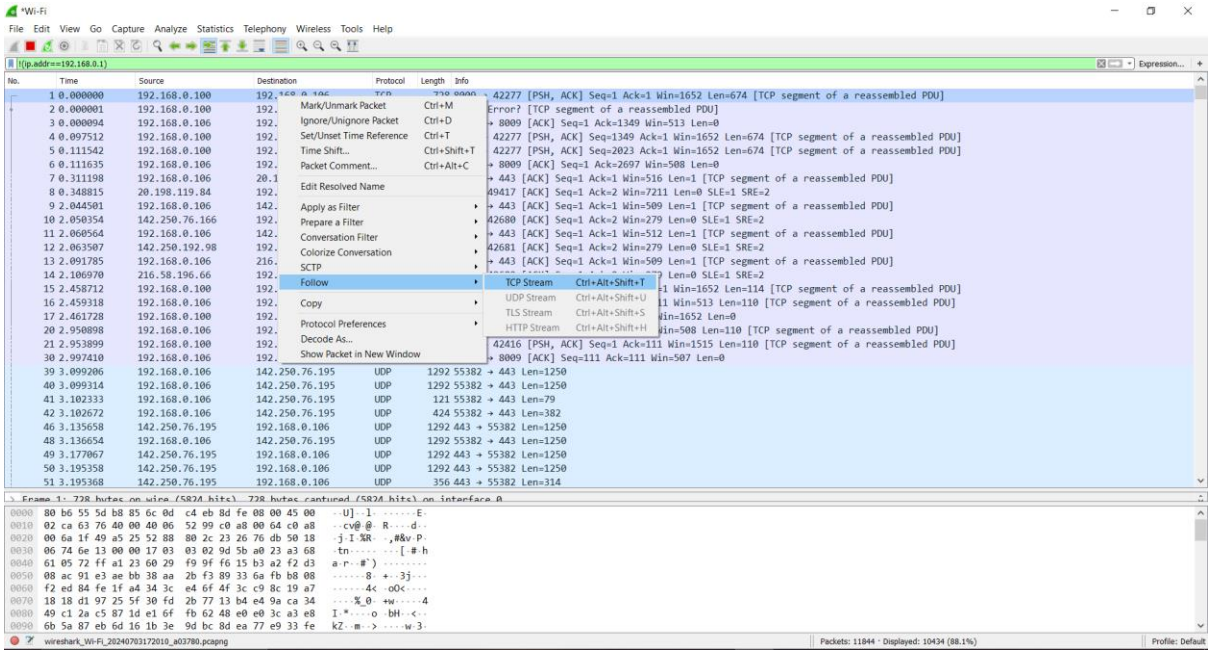
We can also click the Analyze menu and **select Display Filters to create a new filter**



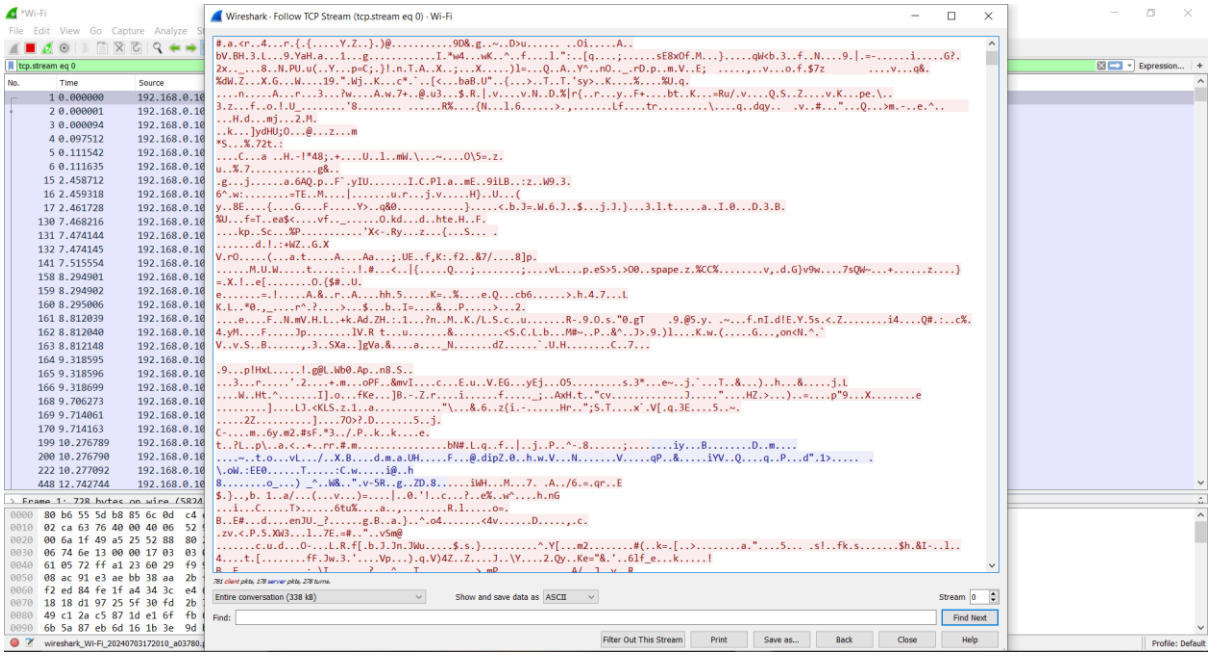
Click on Ok



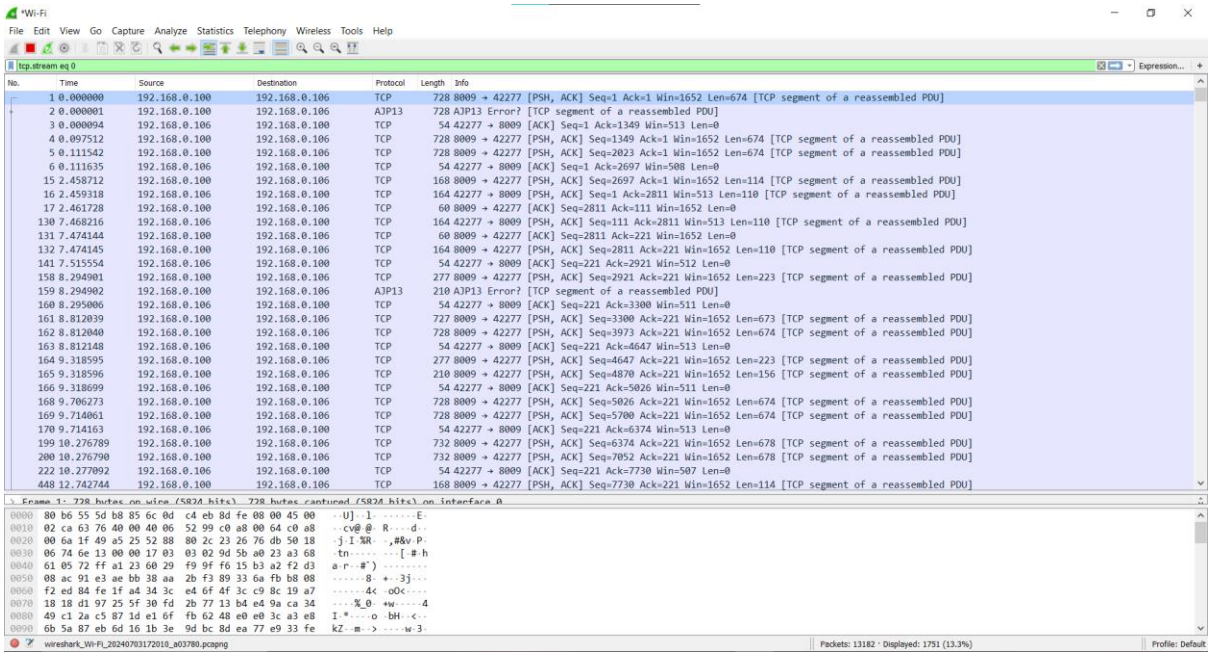
Another interesting thing you can do **is right-click a packet** and **select Follow TCP Stream.**



You'll see the full conversation between the client and the server.

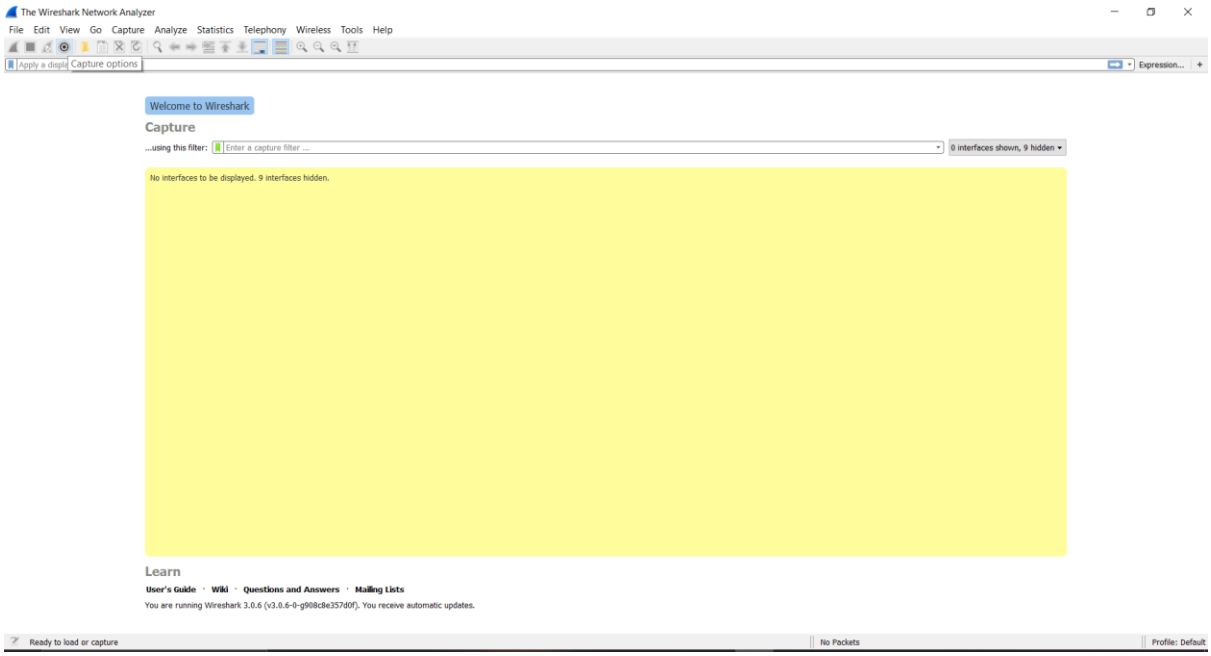


Close the window and you'll find a filter has been applied automatically — Wireshark is showing you the packets that make up the conversation

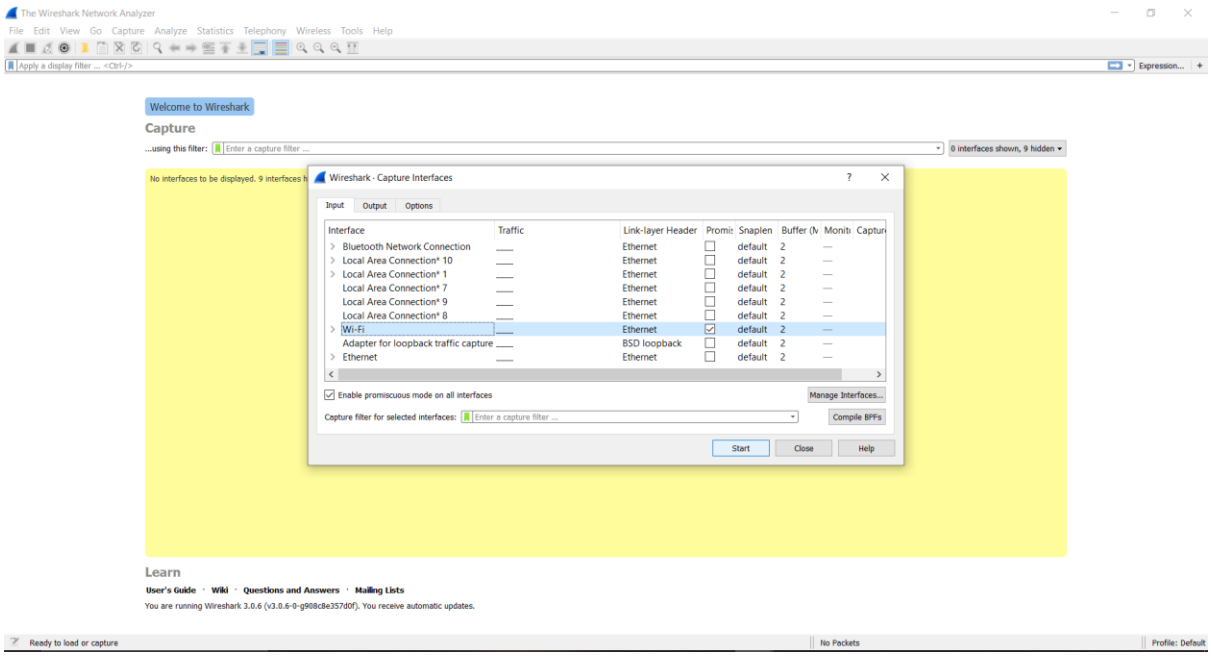


Step 1: Exploring Wireshark

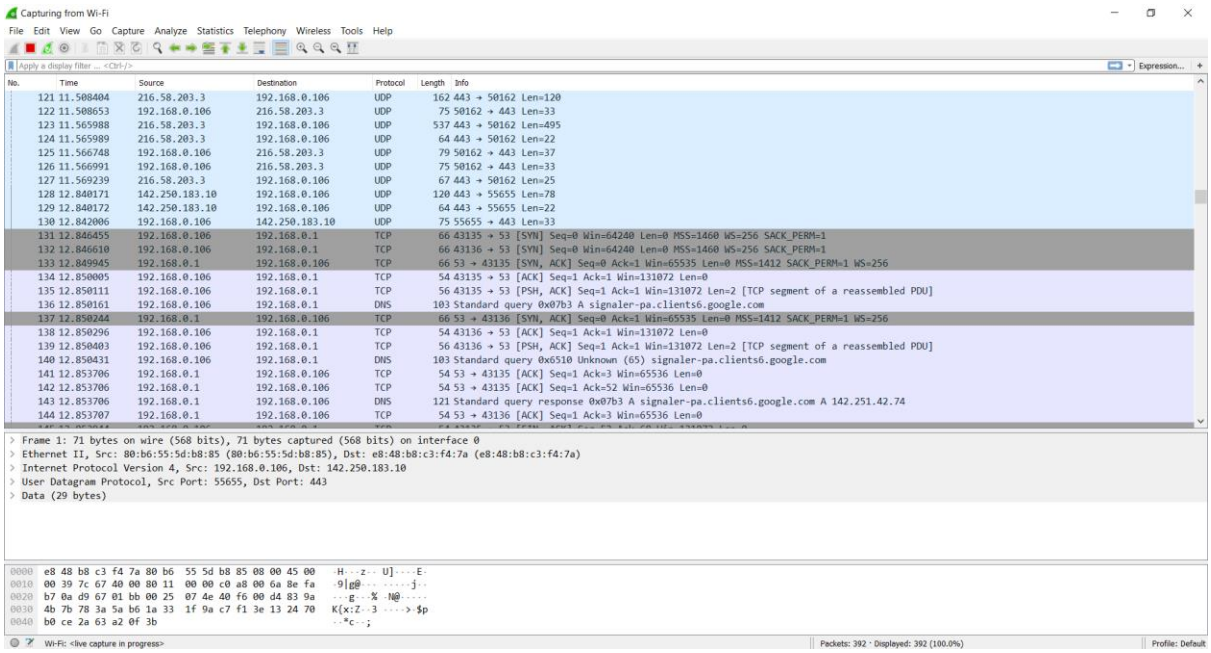
- On menu bar **select Capture Option**



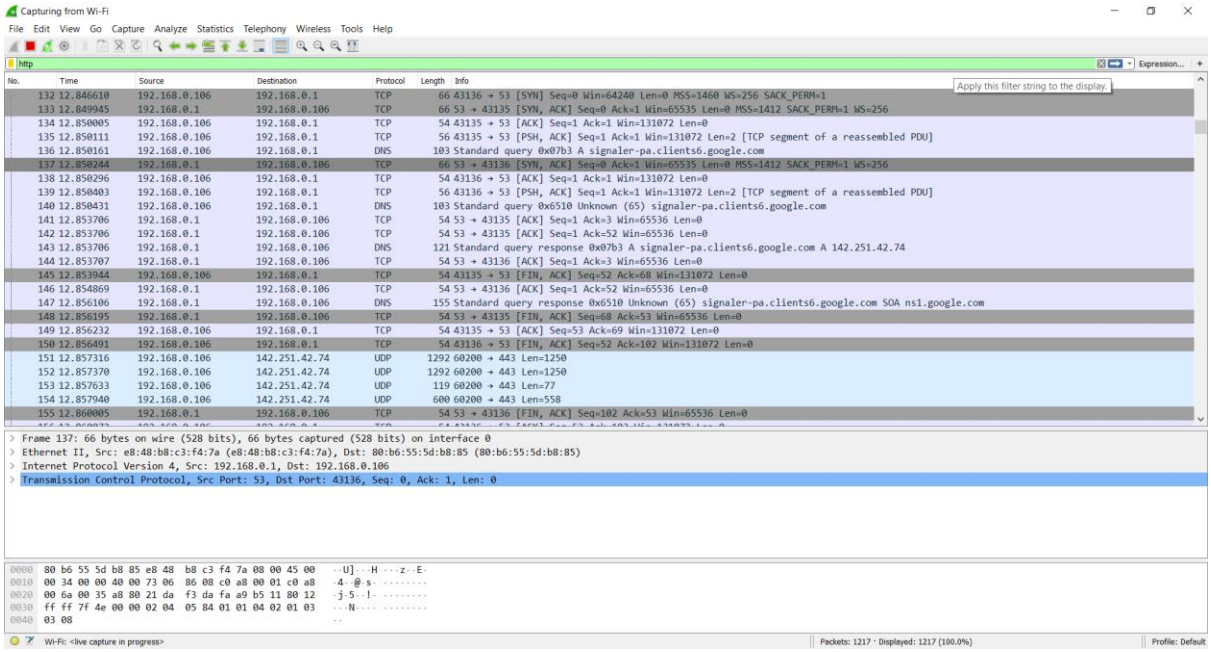
- Select Once you **click on start**



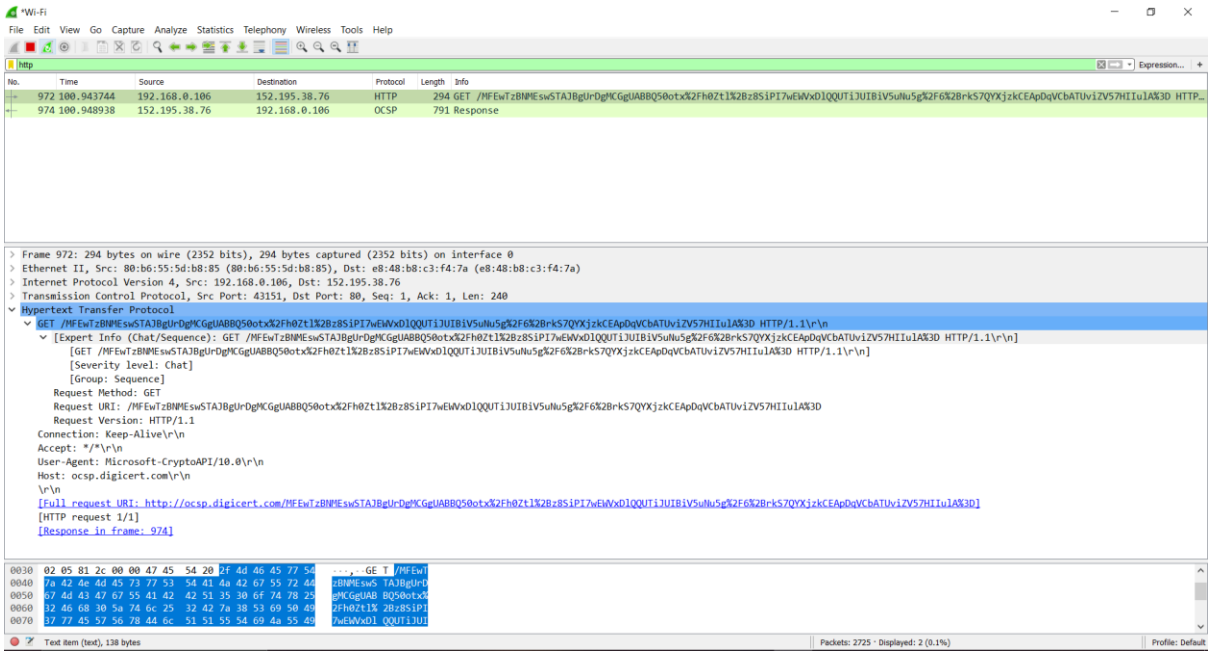
- Wireshark starts to capture the packets on that interface.



Step 2: Filter packets with HTTP protocol

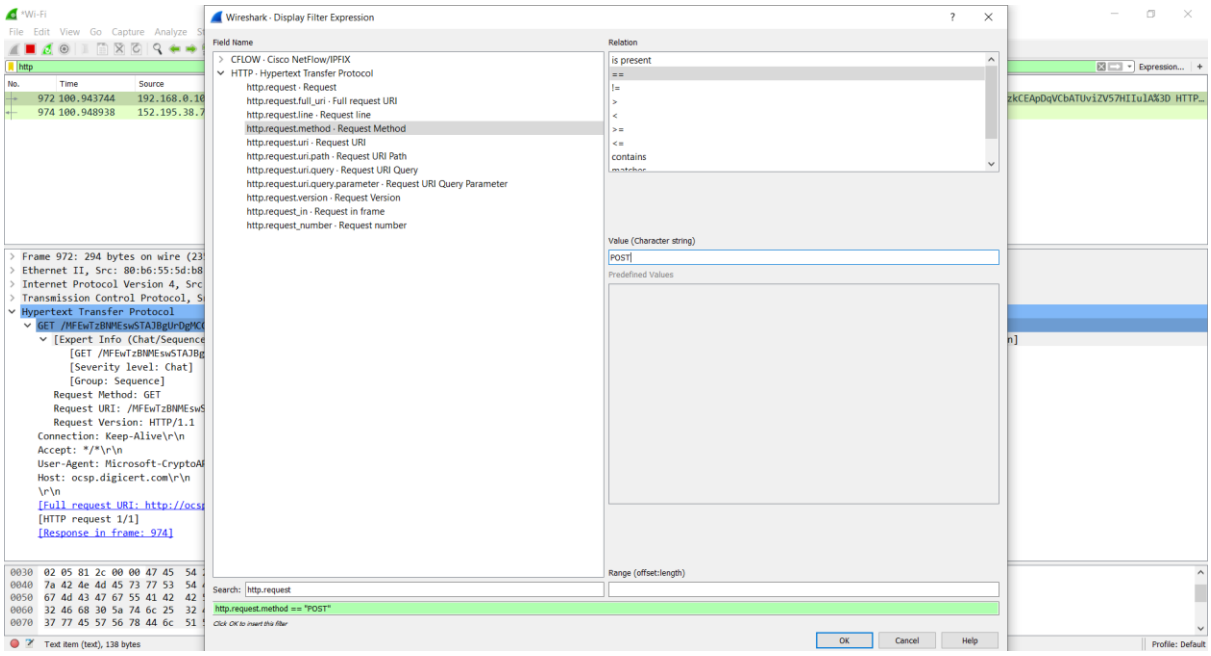


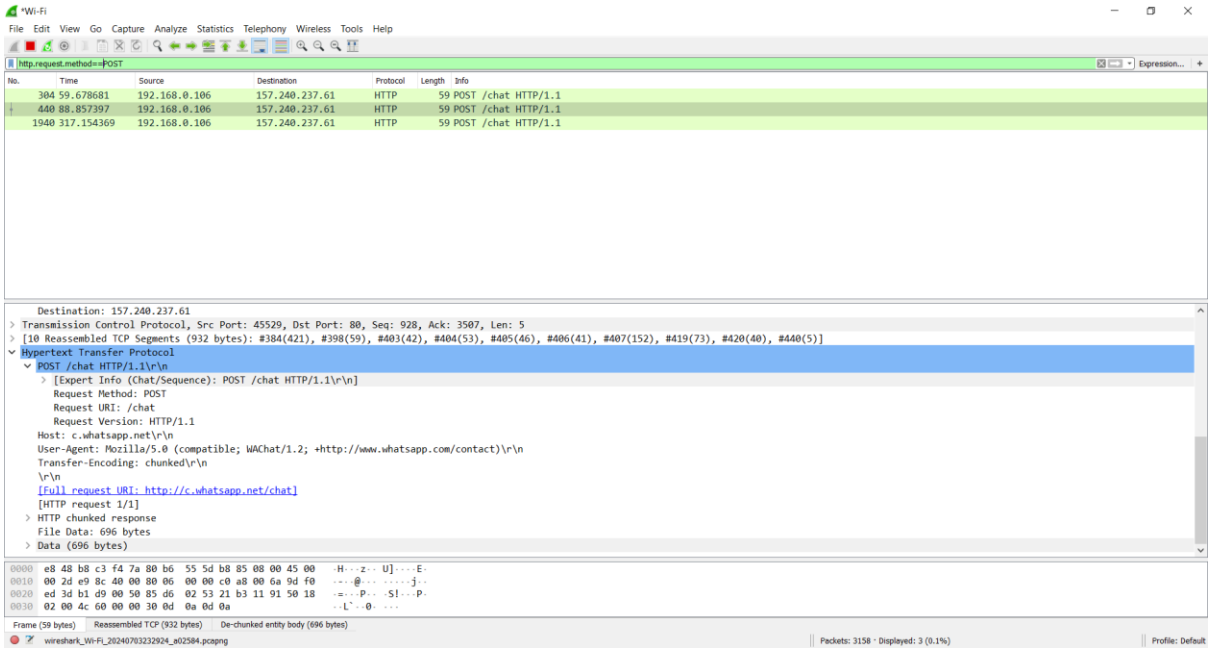
- A file with only text:
  msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?0a9109c2b28701dc



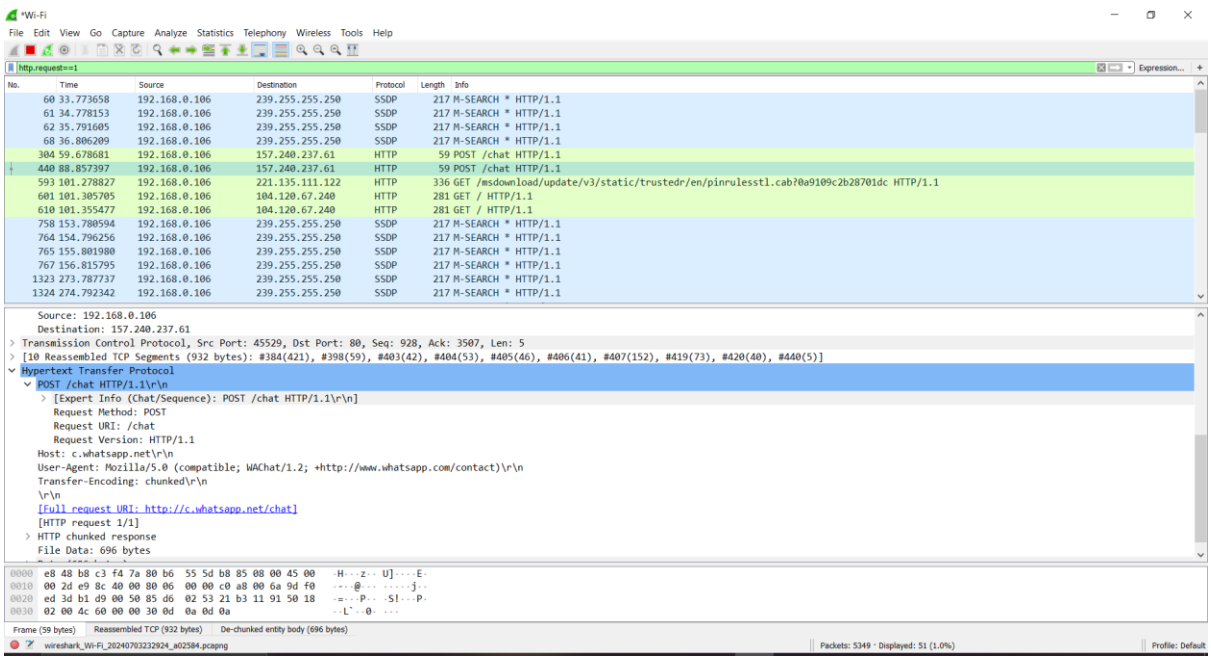
Step 3: Applying different filters using expressions.

- Filtering HTTP POST request
- **Click on Expression** and Select the following and **Click on OK**





- **Filtering HTTP REQUEST==1**



Practical: 5

Aim: Using Data Acquisition Tools [ProDiscover].

Writeup:

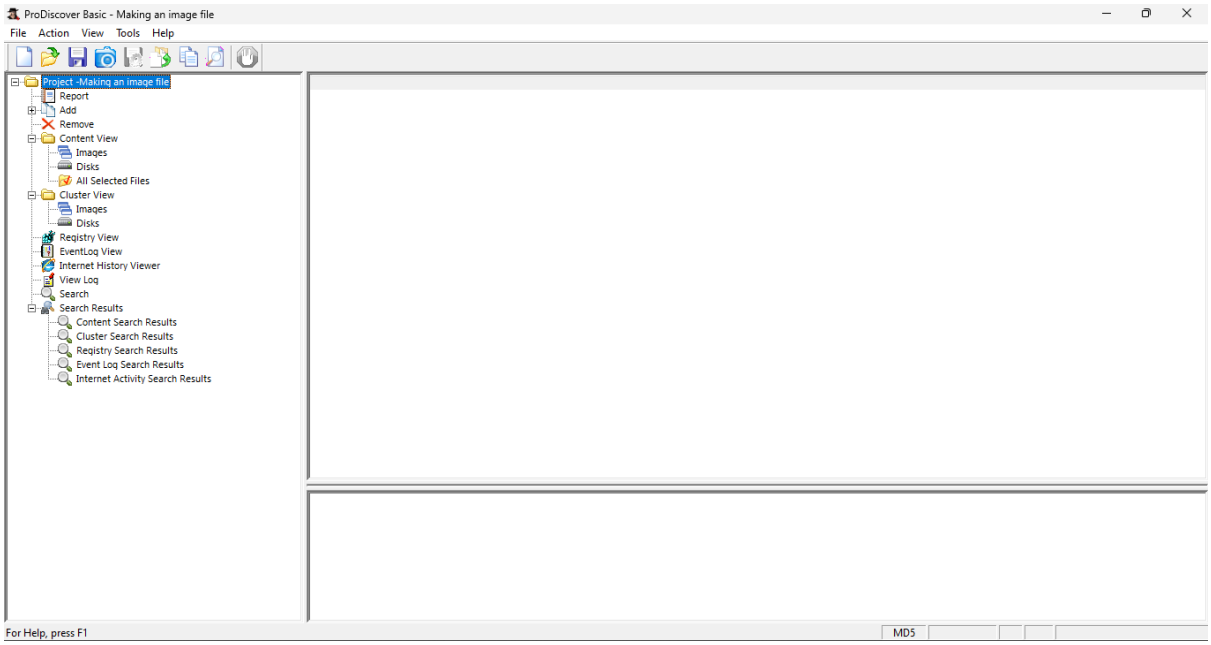
Tasks to be performed:

- Creating a New Project
- Save a project
- Preview a directly connected evidence drive
- Conducting Live Preview of a Remote Disk
- Capture an image of an attached drive
- Capturing Physical Memory
- Add an image file to a project
- Restore an Image to directly connected drive

Step 1: Creating a New Project

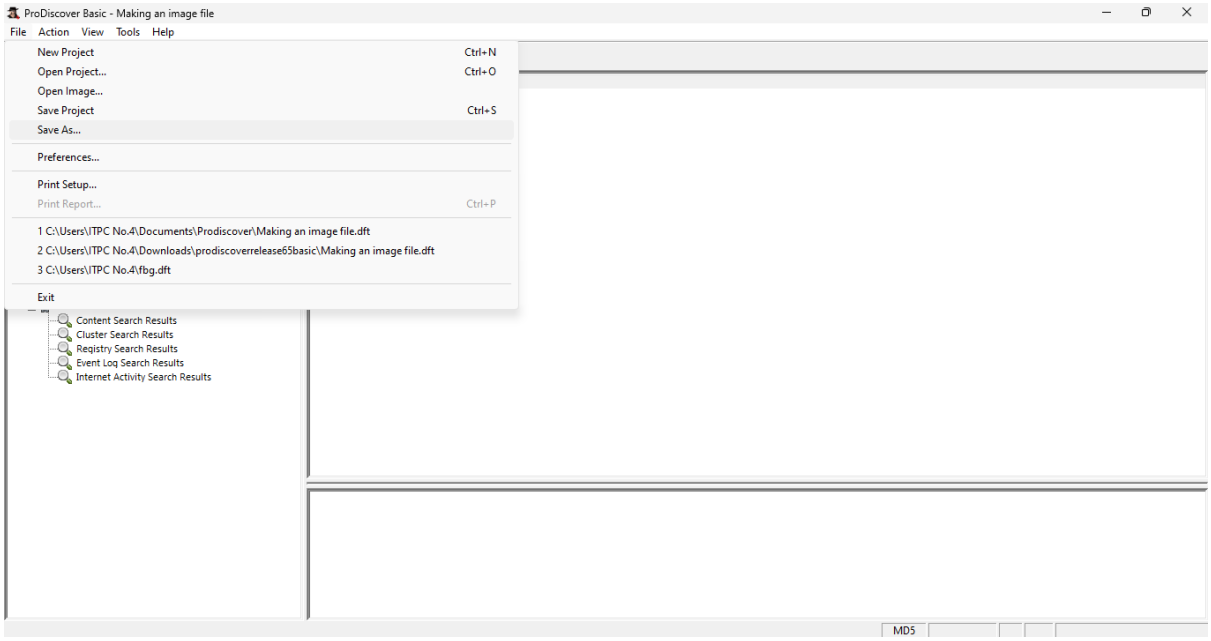
- Start **Prodiscover** and **Type Project Number** and **Project File Name** and **Click on Open**

- Here We Can See **ProDiscover Create New Project**

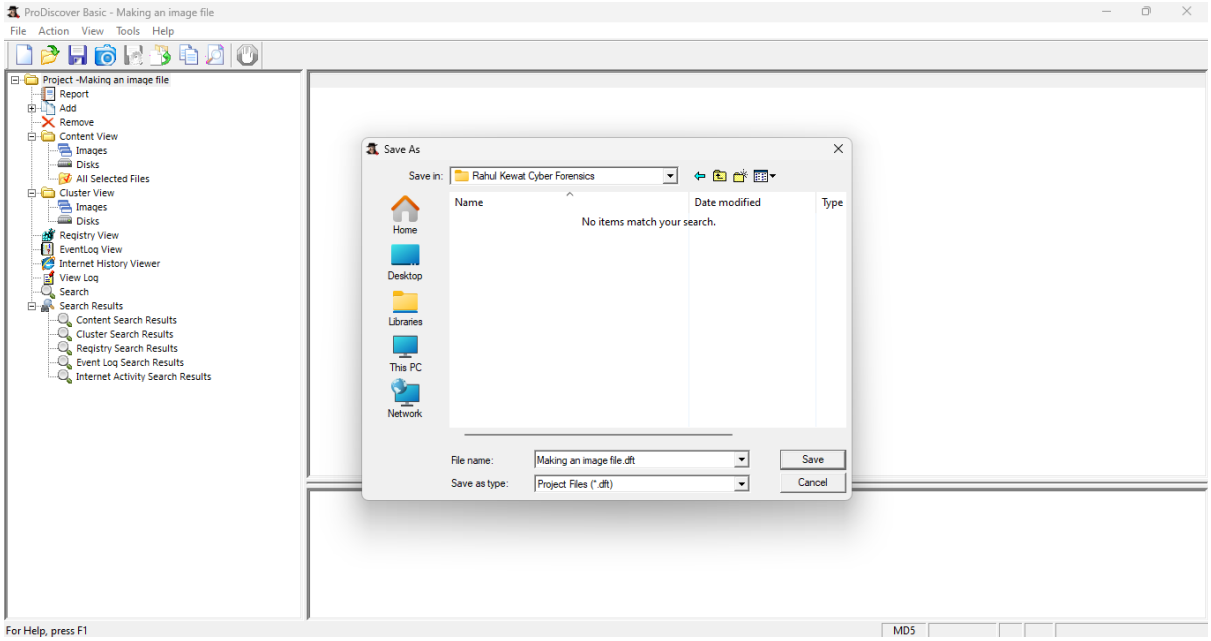


Step 2: Saving a project

- **Click on File** and **Select Save As..**

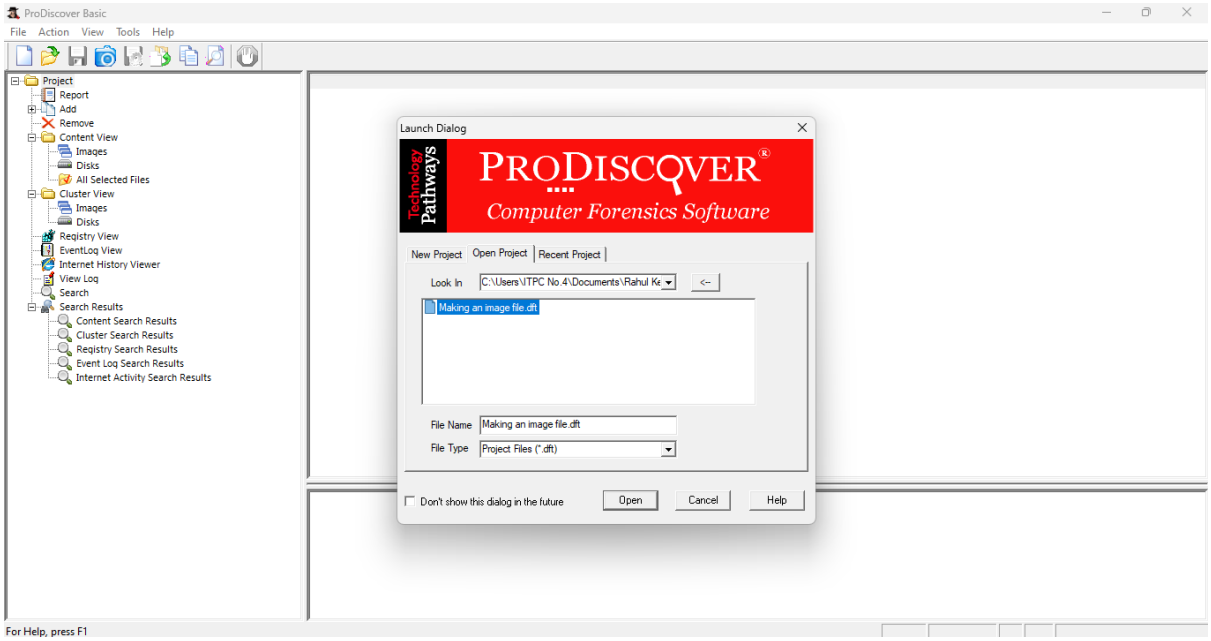


- **Select** the **destination path** and **click** the **Save button**



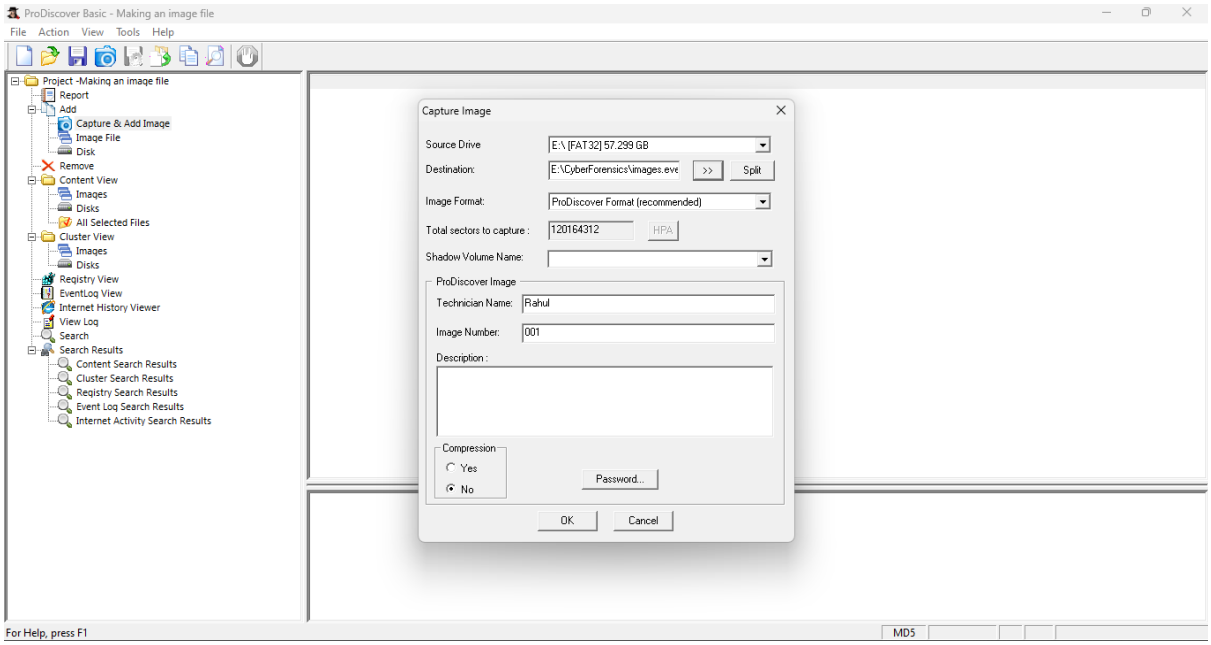
Step 3: Preview a directly connected evidence drive

- **Launch ProDiscover**
- **Select open project tab option.**
- **Select the project file to open and click Open button**
- **ProDiscover opens the project file and generates a template report in the work area**

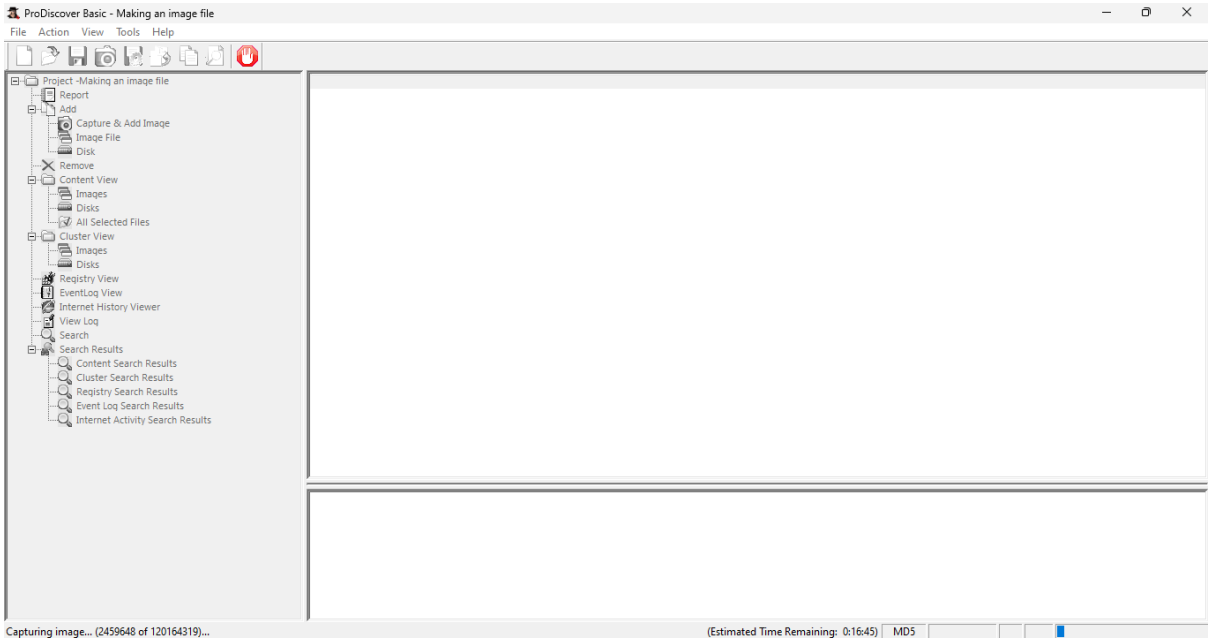


- **Under Report, expand Add** and **click on Capture & Add Image.**
- **Give Destination, add Technician Name** and **image number and click on OK**

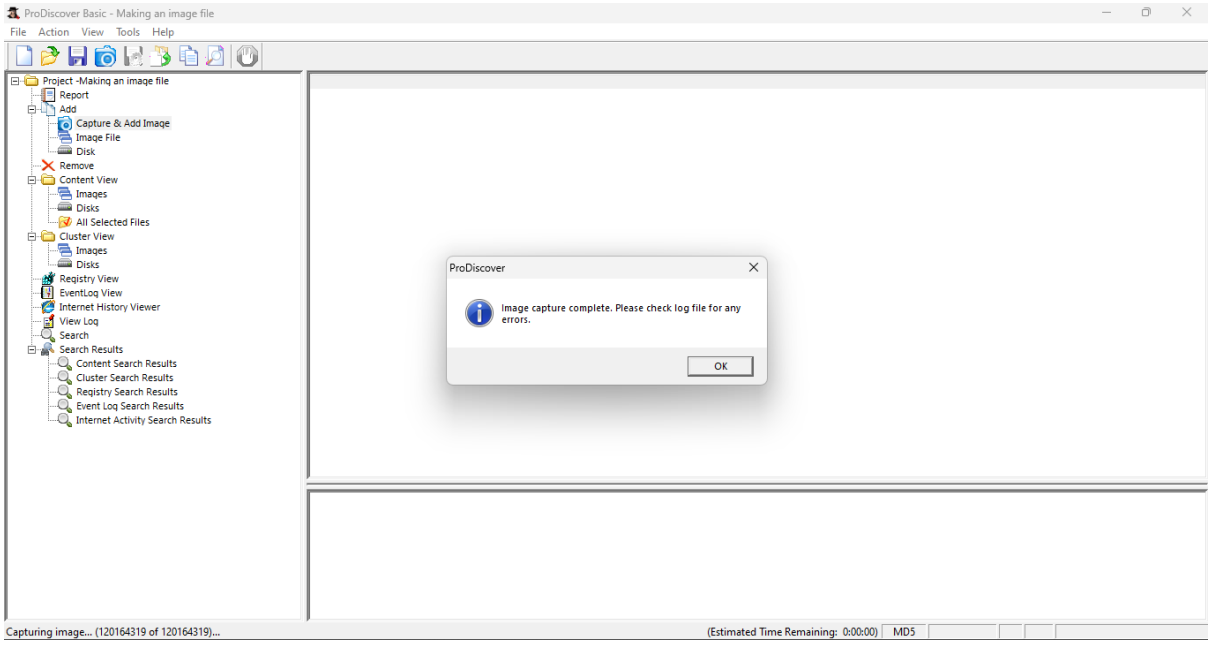
Note: Use Pen drive for Source Drive and and Create or Select File in Physical C-Drive for Destination



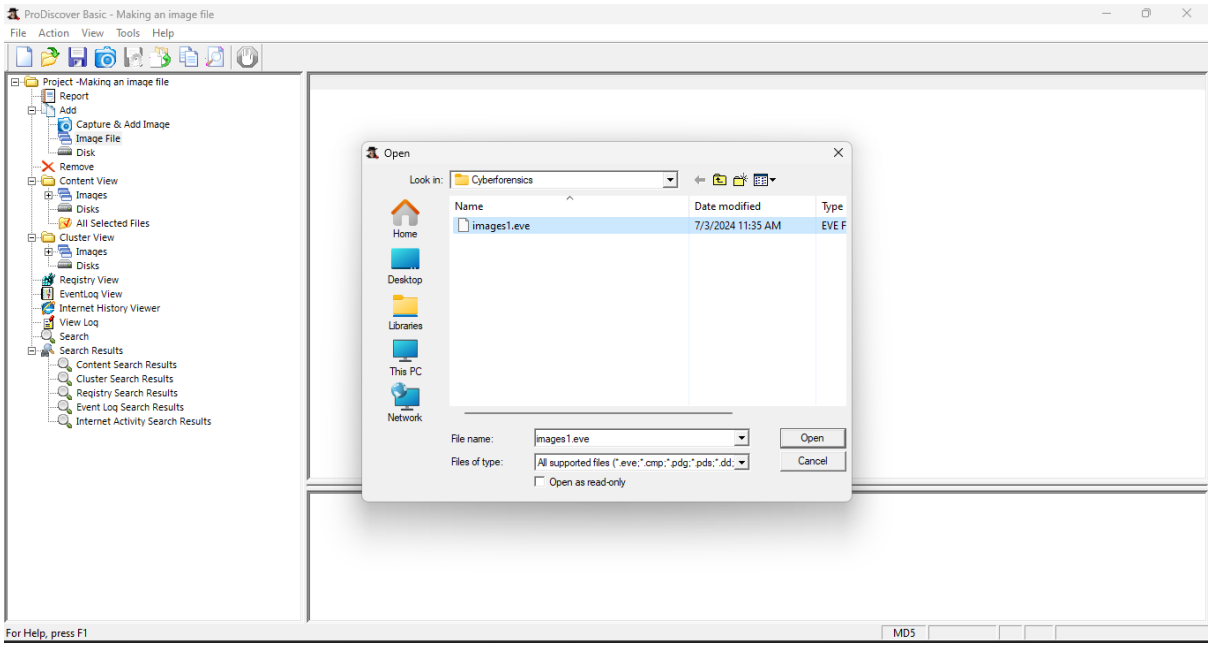
- Image Capture Process Start



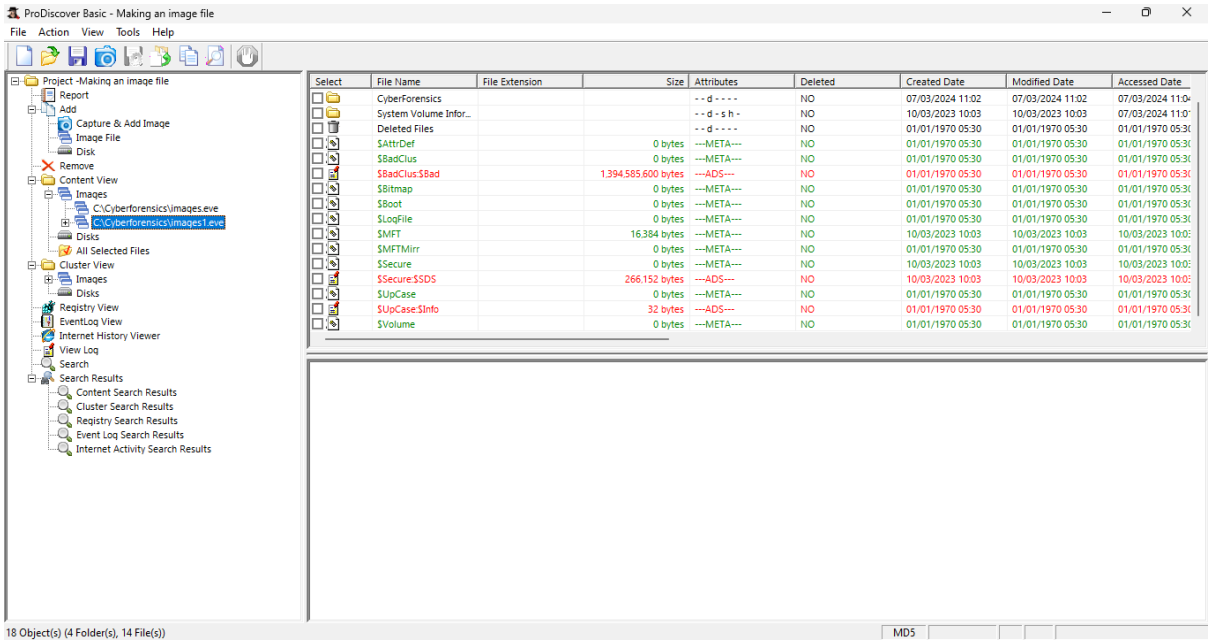
- Once the **image capturing** is completed, **click on OK**



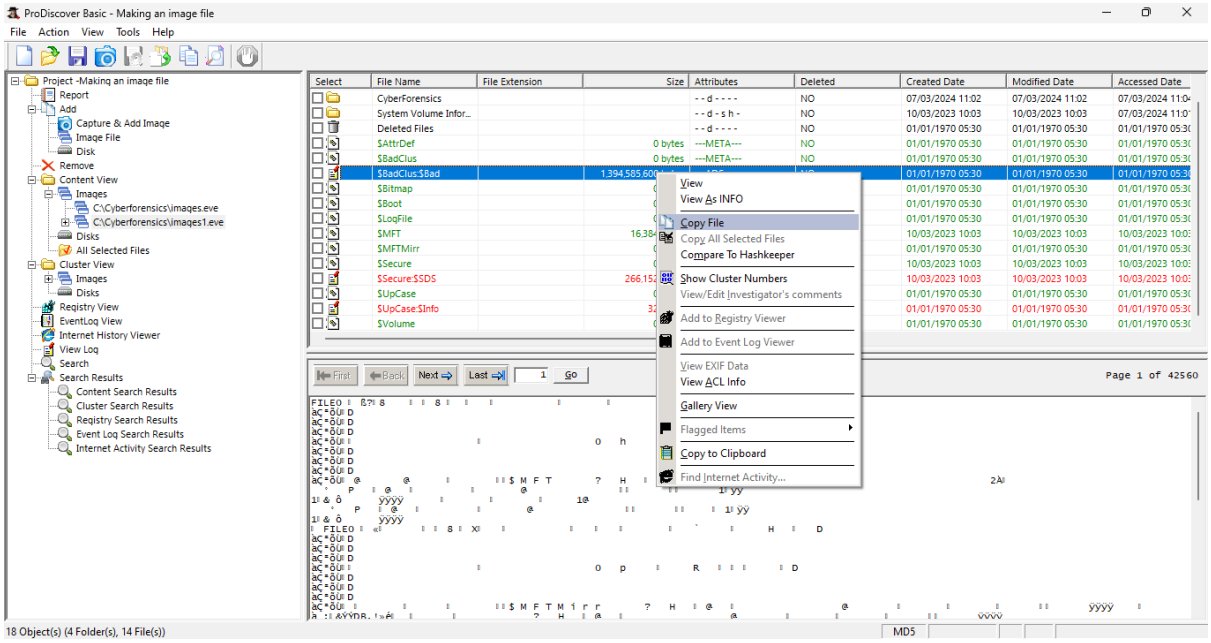
- **Under Add, click on Image File, click on the image** that you **created** and **click Open**



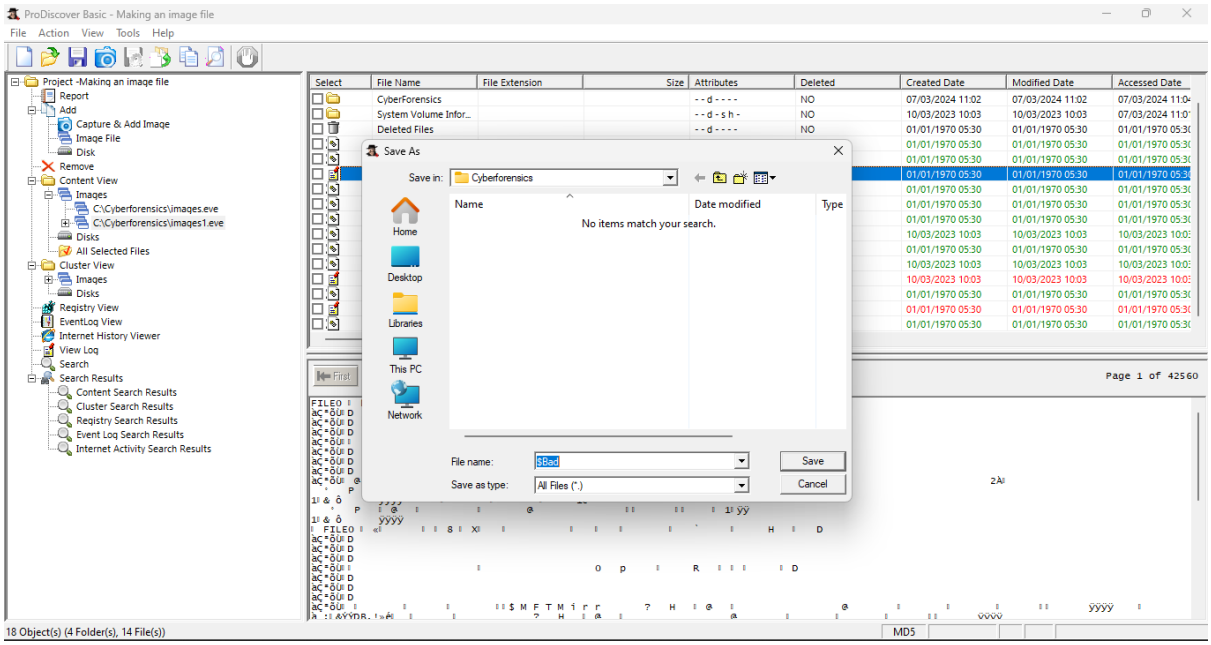
- The image file will get added. Then under **Content view, click on images** and **select the image.**



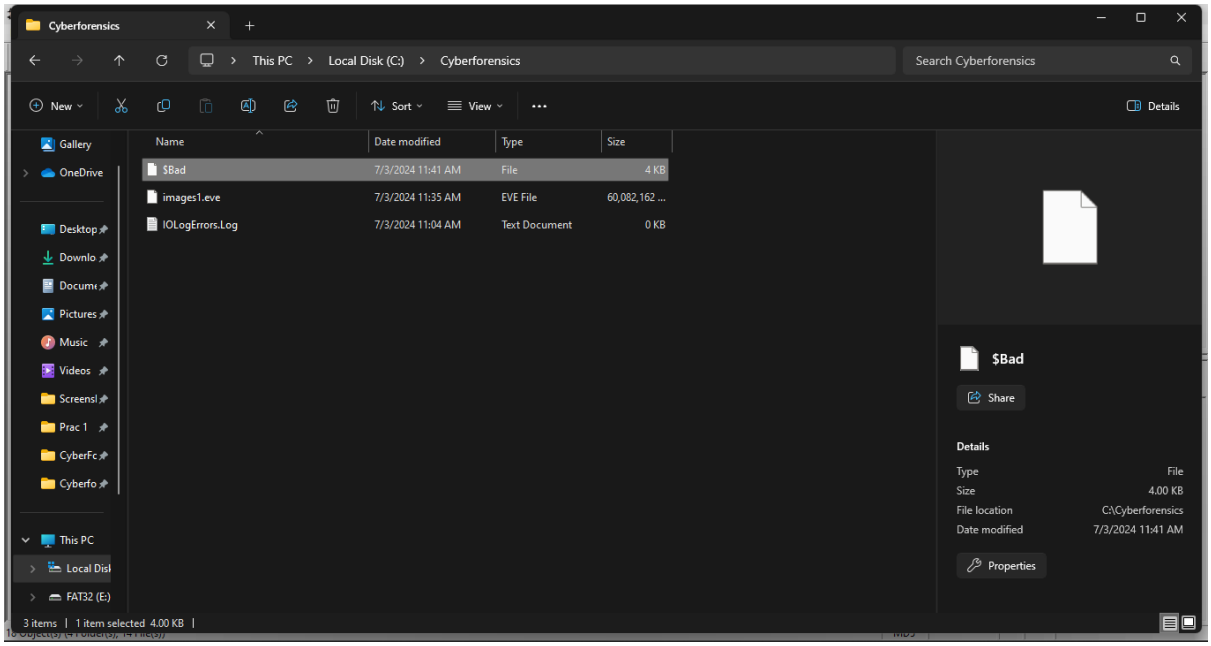
- **Right click on deleted file, either view it or copy the file to a folder.**



- **Save the file**



- Navigate to the folder and there you can see the deleted file.



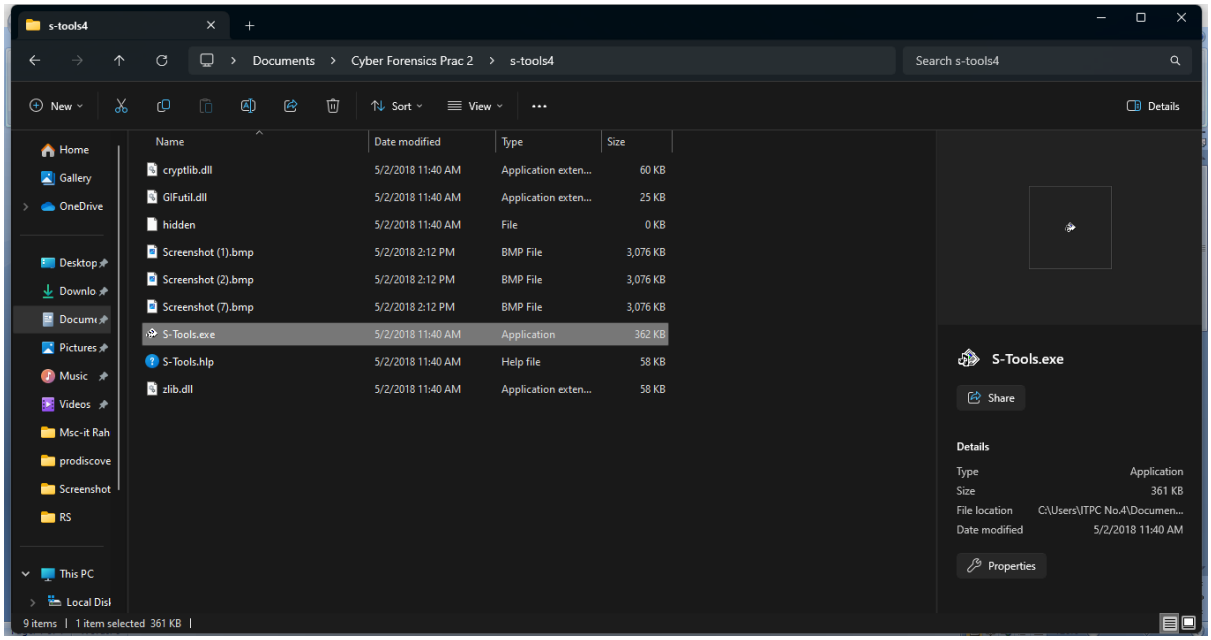
- You can view the deleted file once saved in a folder.

Practical: 6

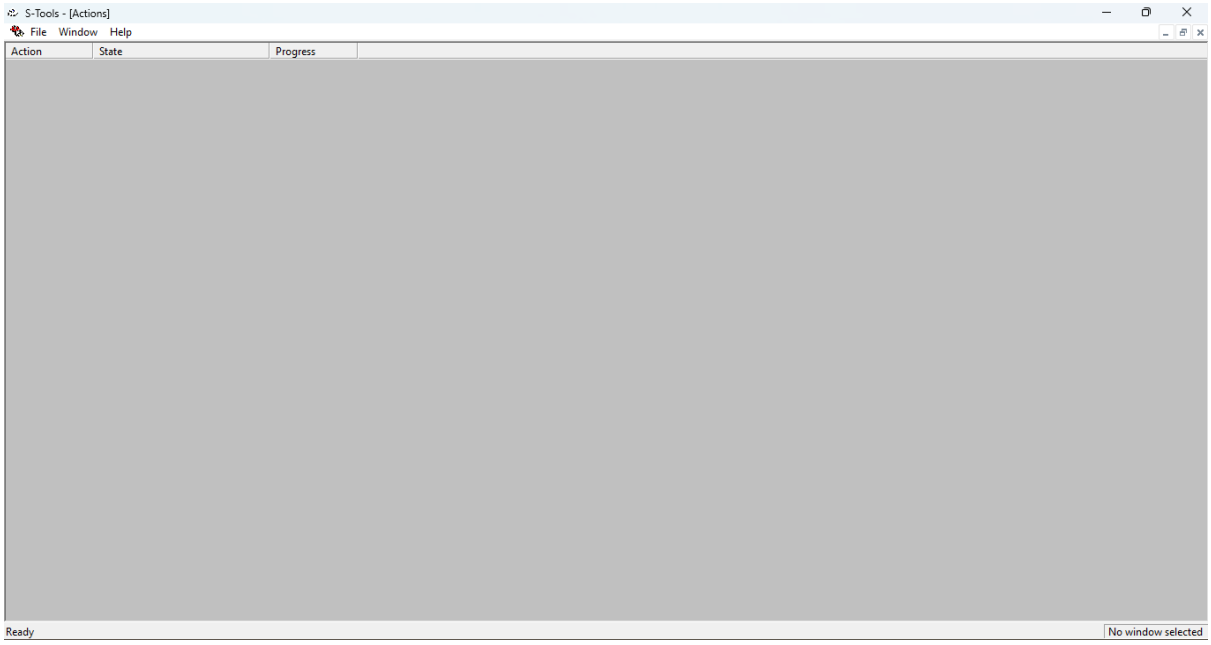
Aim: Using Steganography tools [S-Tools].

Writeup:

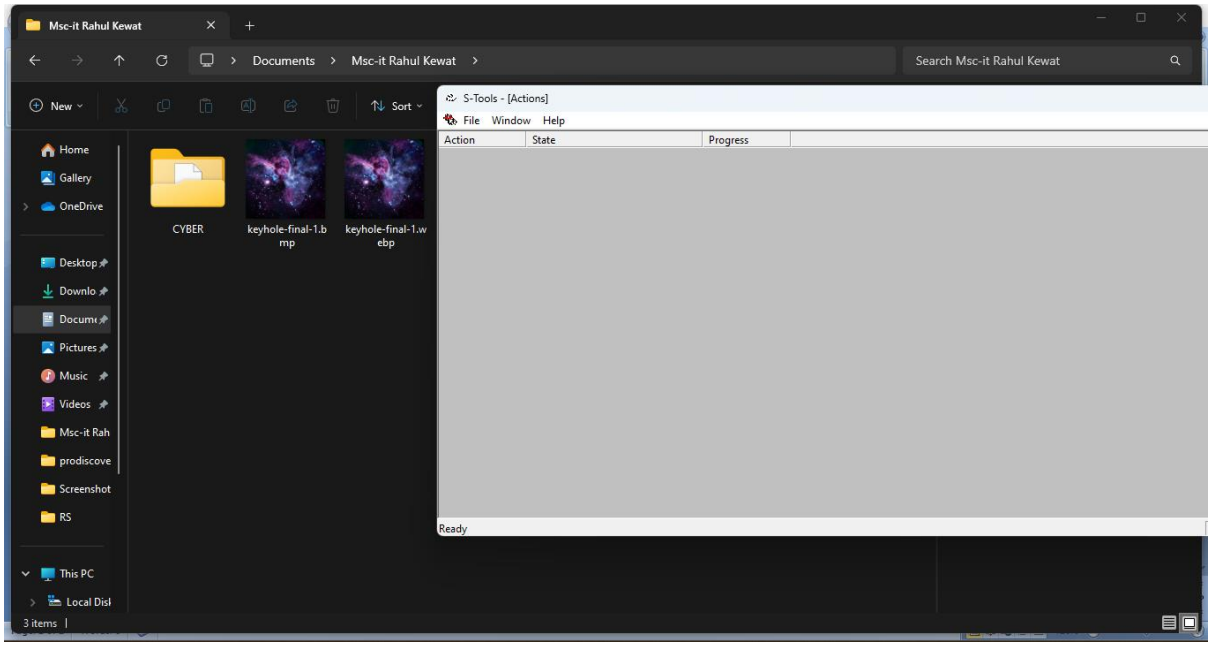
Step 1: Select the **S-Tools.exe file** and open the **steganography** software tool**.**



- S-Tools Window Open

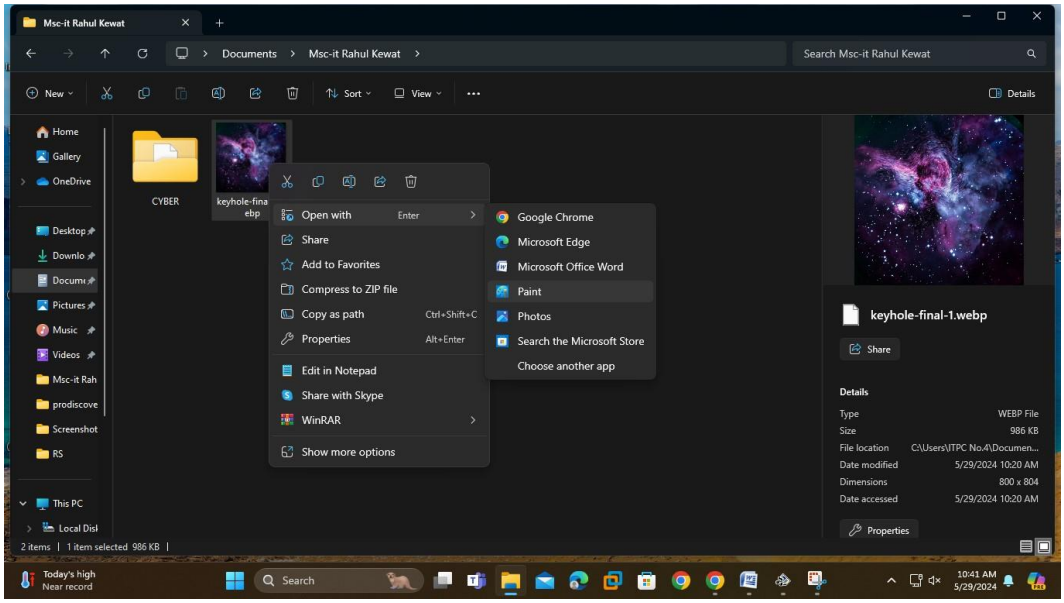


Step 2: With both the working directory and the S-Tools program open minimize both windows and place side-by-side. The S-Tools program is a drag and drop software. The files used to create the steganography file can be dragged from the directory into the S-Tools program.

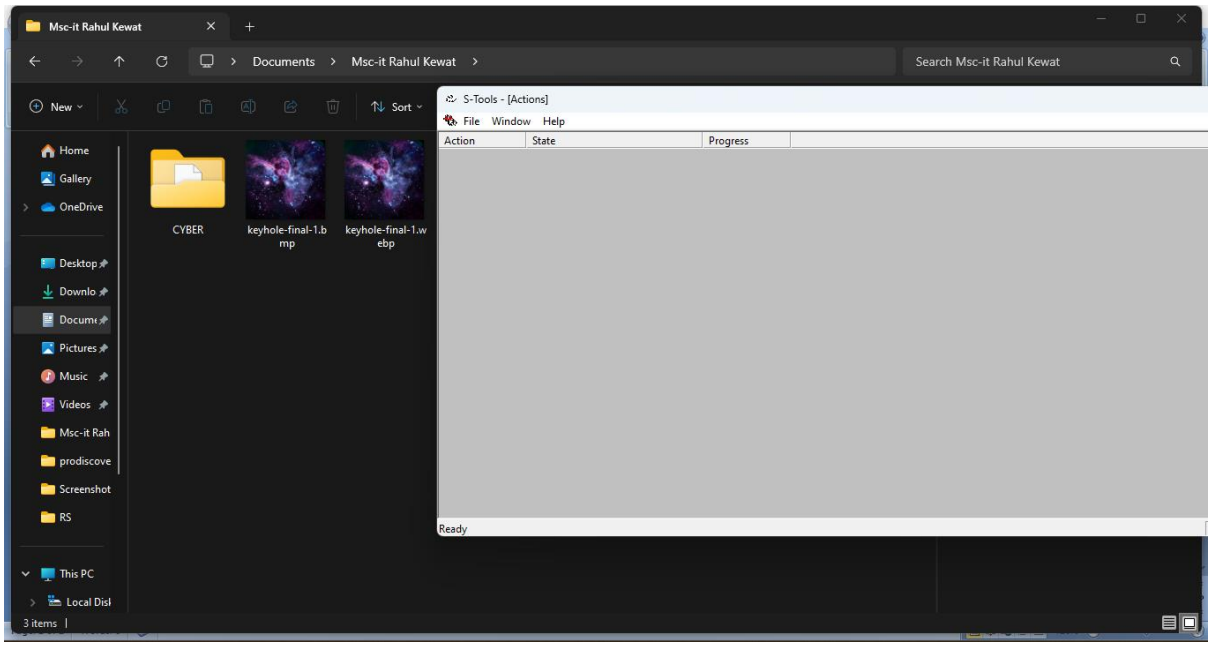


Step 3: If your image is in .jpg format, convert it to .bmp format by doing the following steps

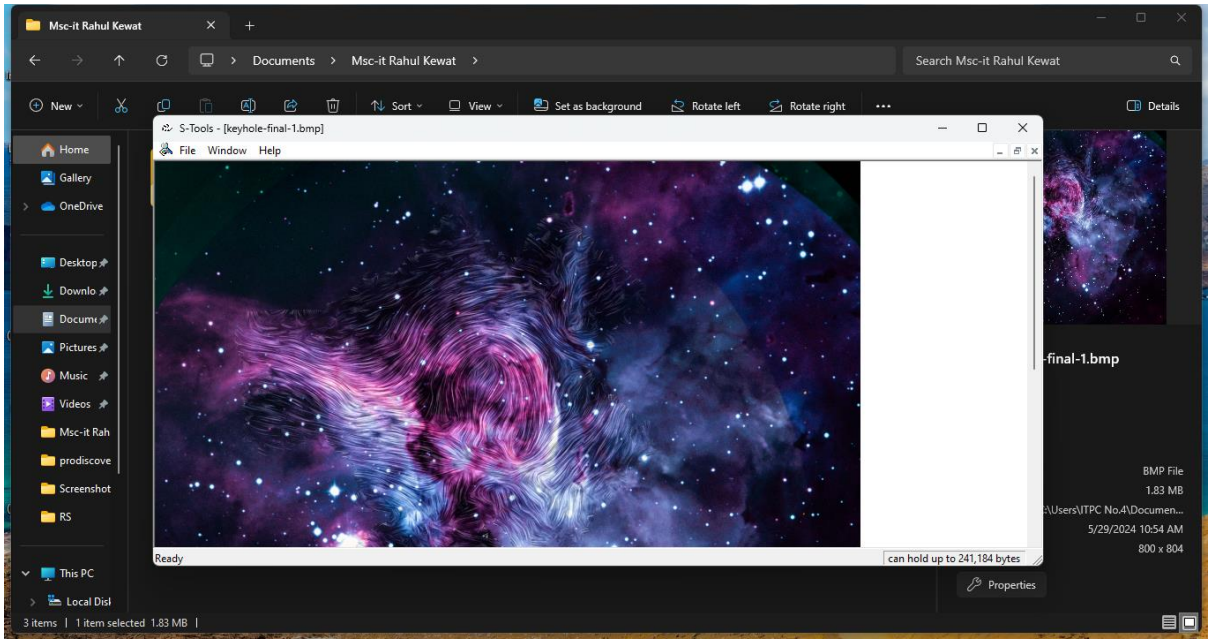
- Open the Selected Image With Paint and Save image in BMP format



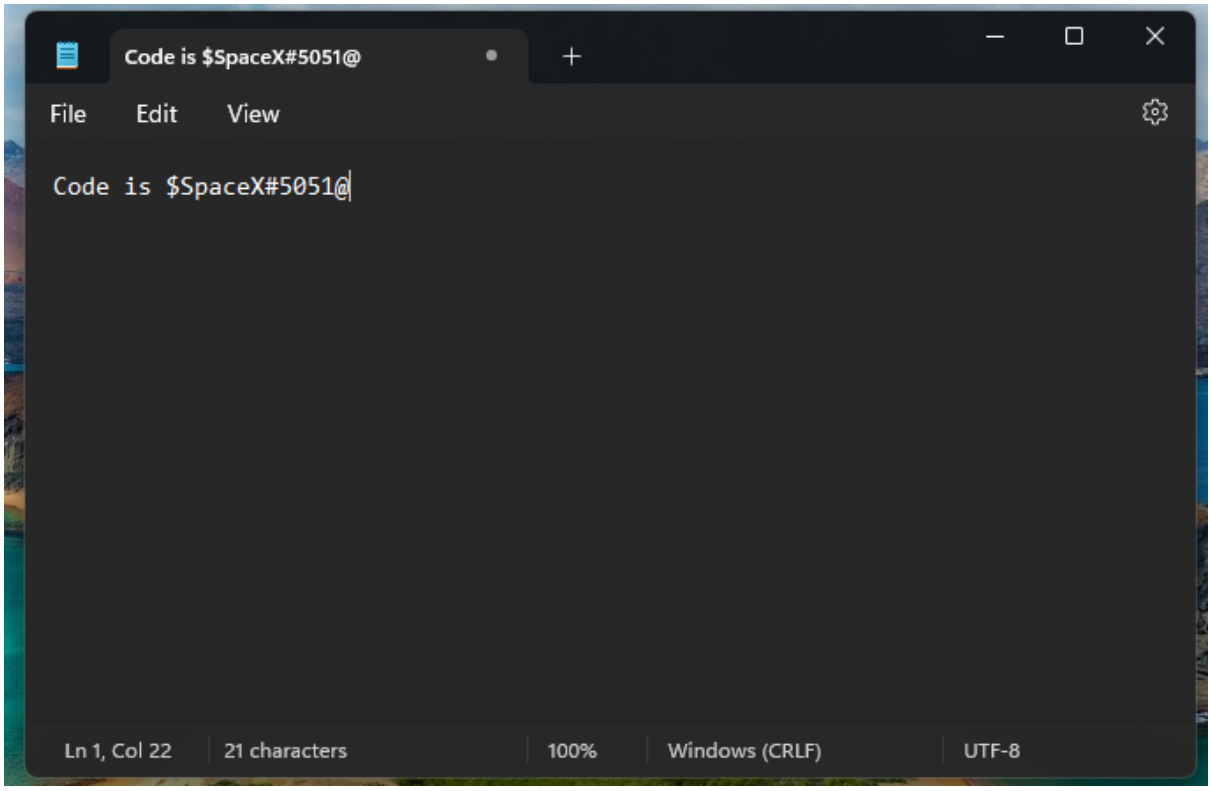
Step 4: The keyhole-final-1.bmp was selected and dragged onto the main window of the S-Tools program.



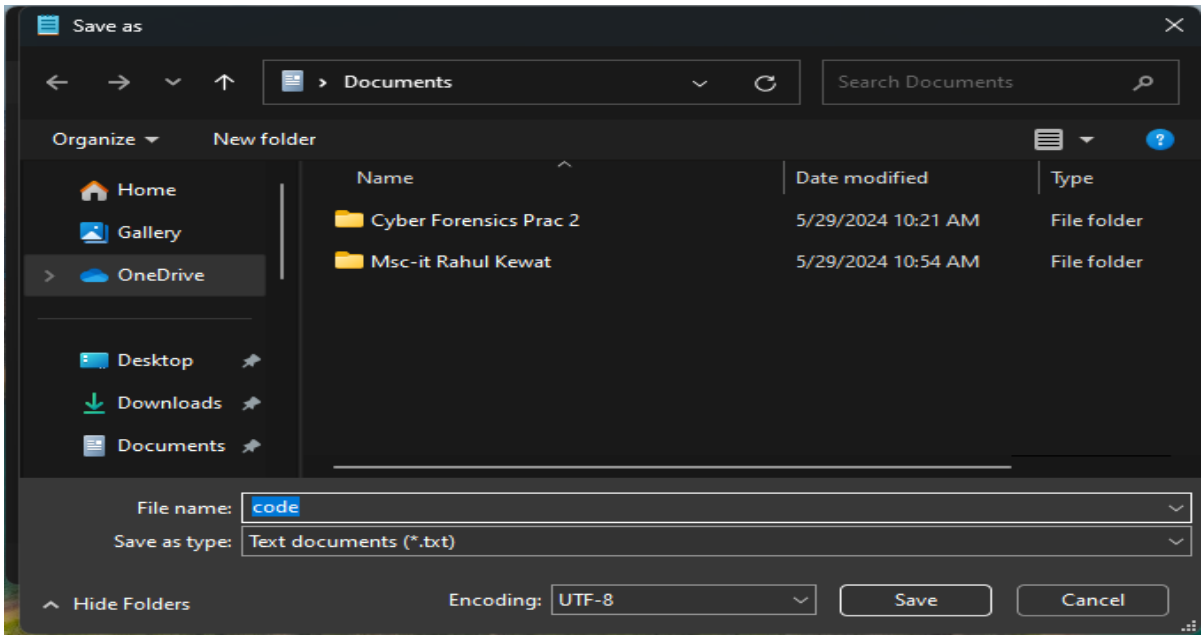
- **The image is opened.**



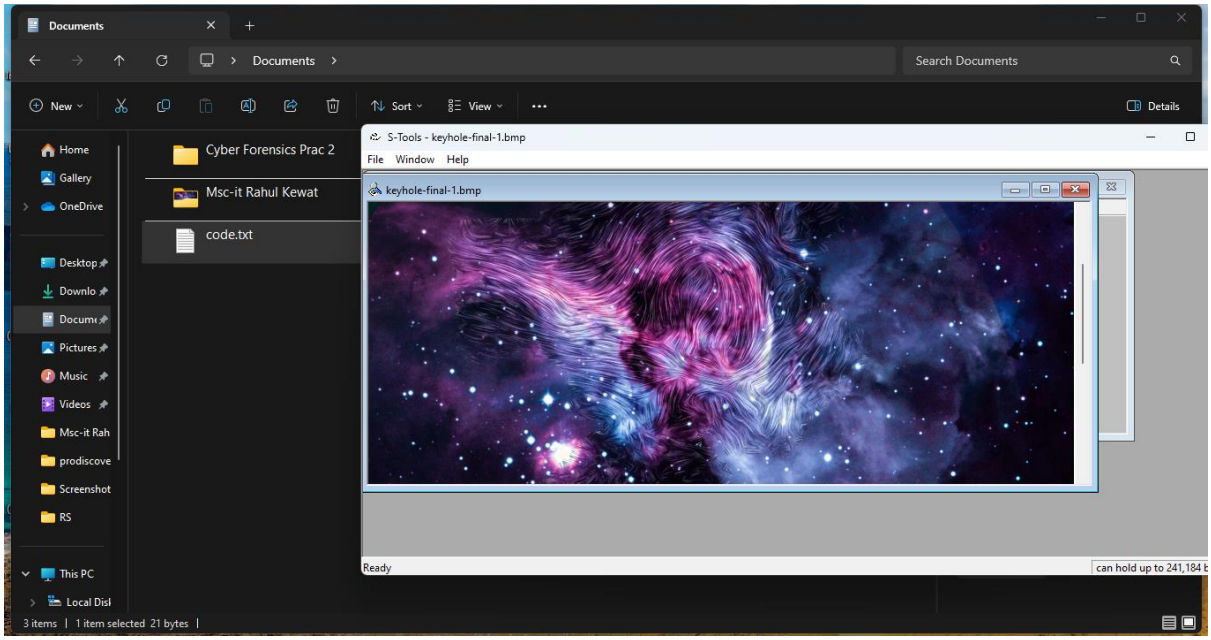
Step 5: Select a file to hide within the base file. If it's not there, create a txt.



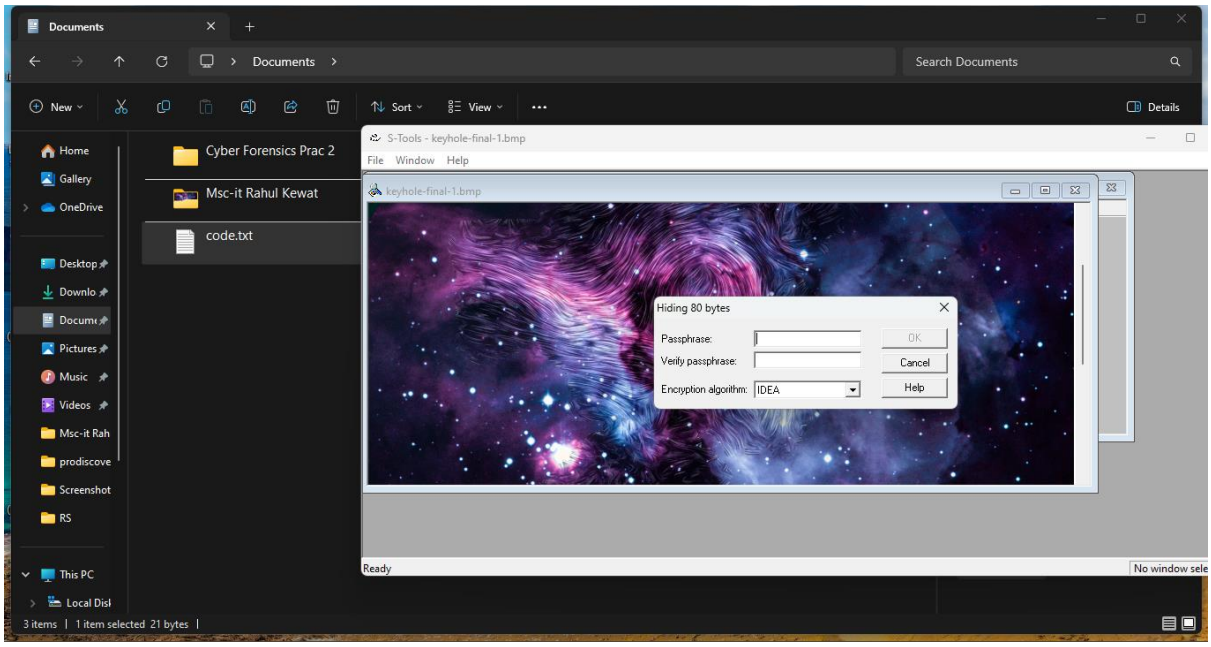
- **Save the file**



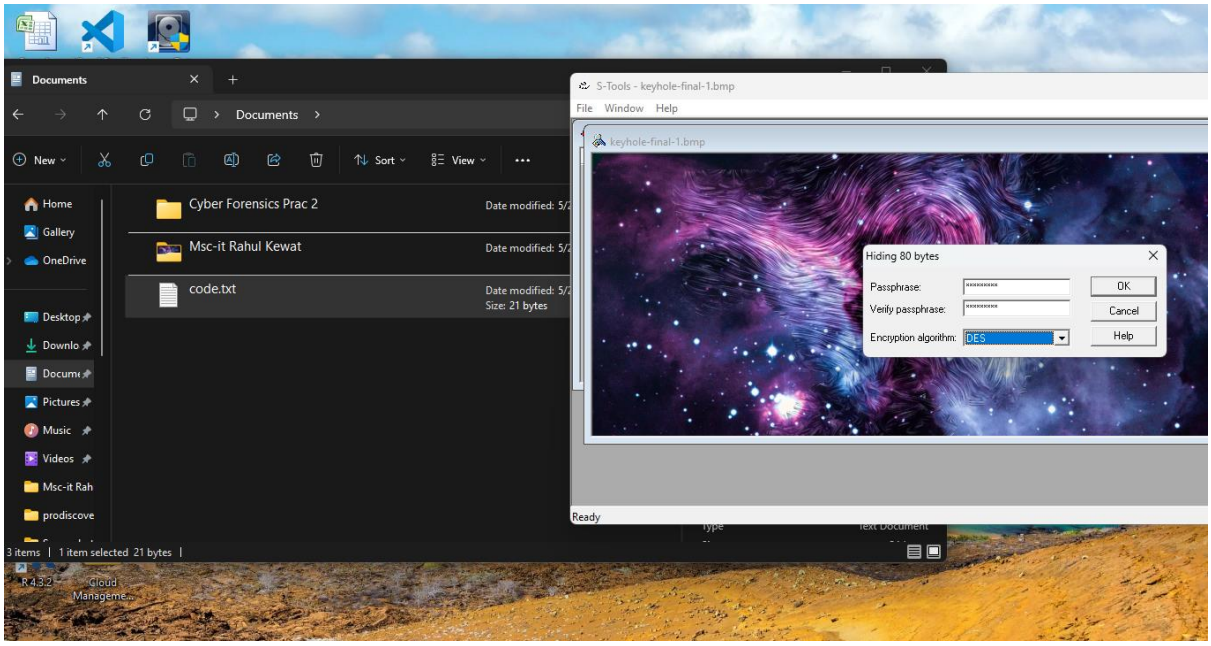
Step 5: The code.txt was selected and dragged onto the main window of the S-Tools program.



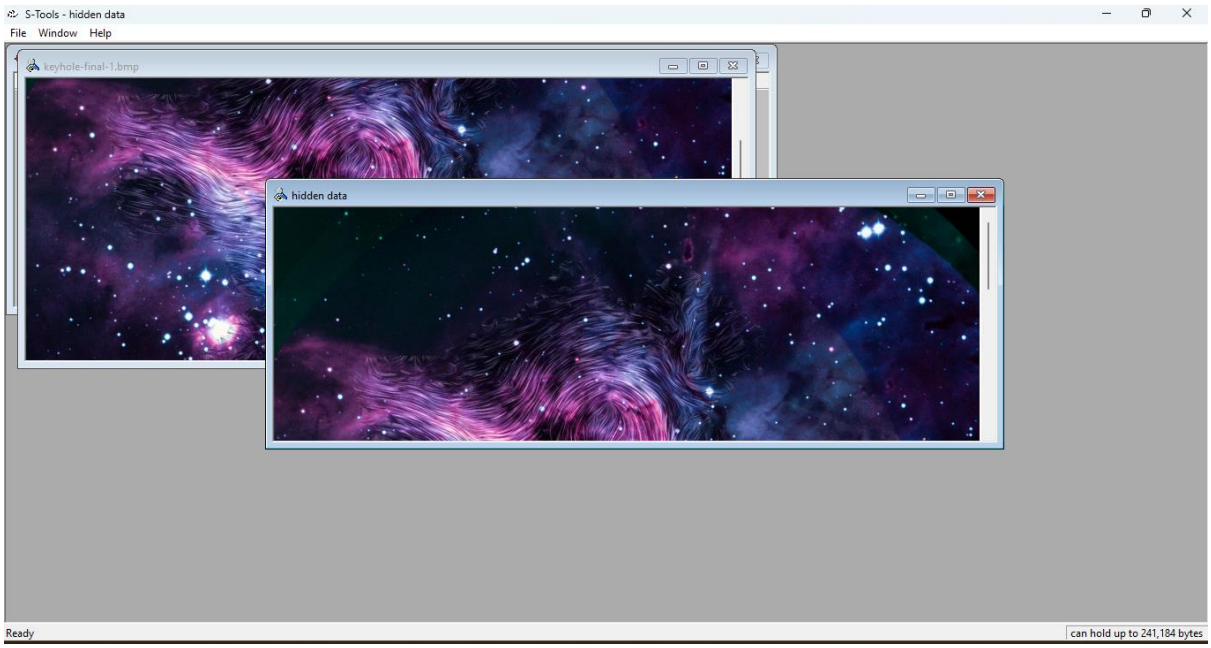
- After Dragged code.txt file onto main window of the S-Tools A dialogue box will appear asking the user to enter and verify a passphrase. Additionally, the user will have to select an encryption algorithm.



- Enter a **passphrase** in both the **passphrase** and **verify passphrase text boxes**. And **Click on OK**

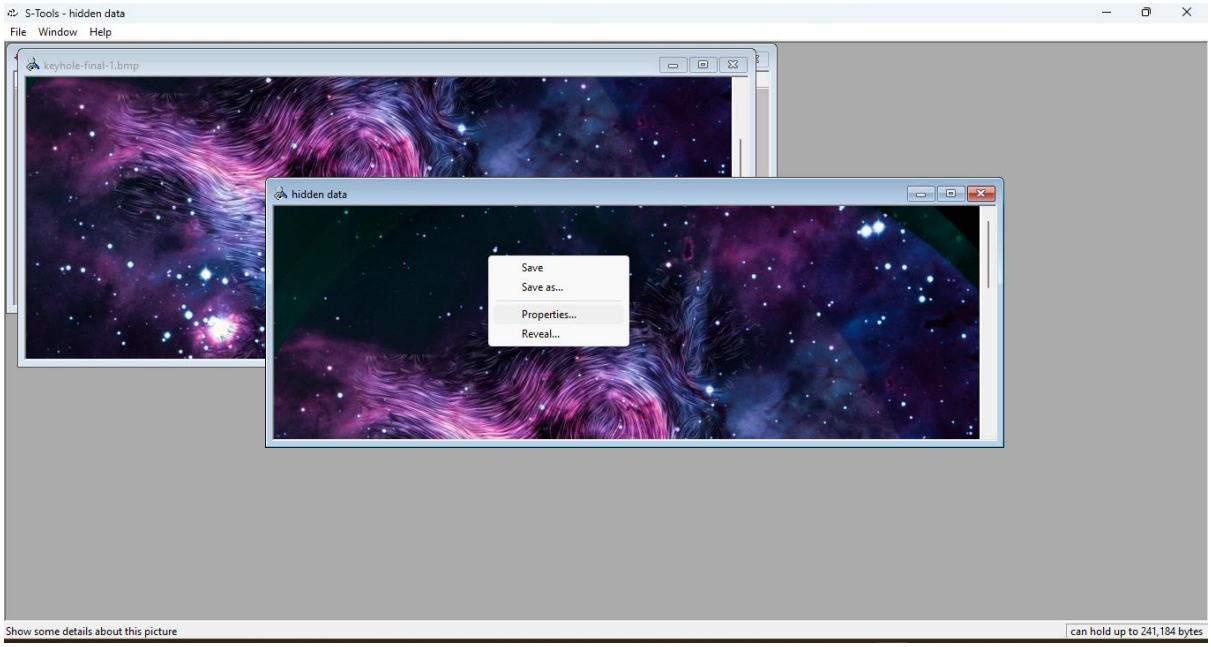


Step 6: The S-Tools main window will appear and a new file will be visible. The name of the file will be called **hidden data by default.**



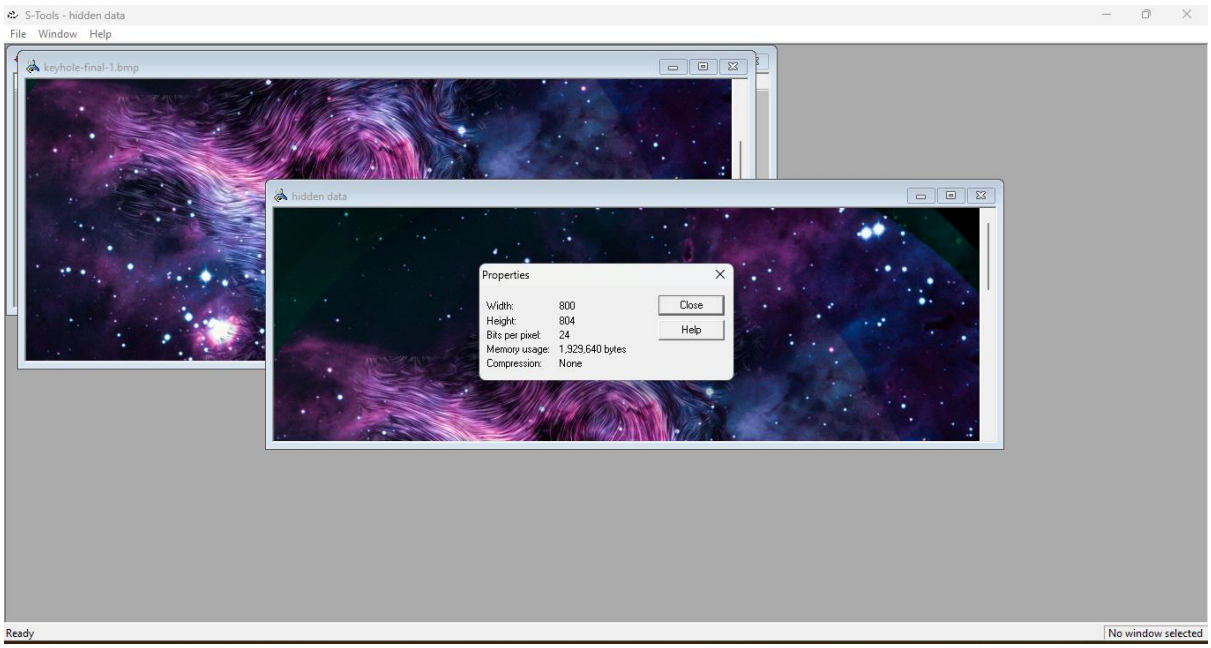
Step 7: Place the cursor on top of the hidden data image and select the right mouse button. The user will have four options available to them

- Save
- Save As
- Properties
- Reveal

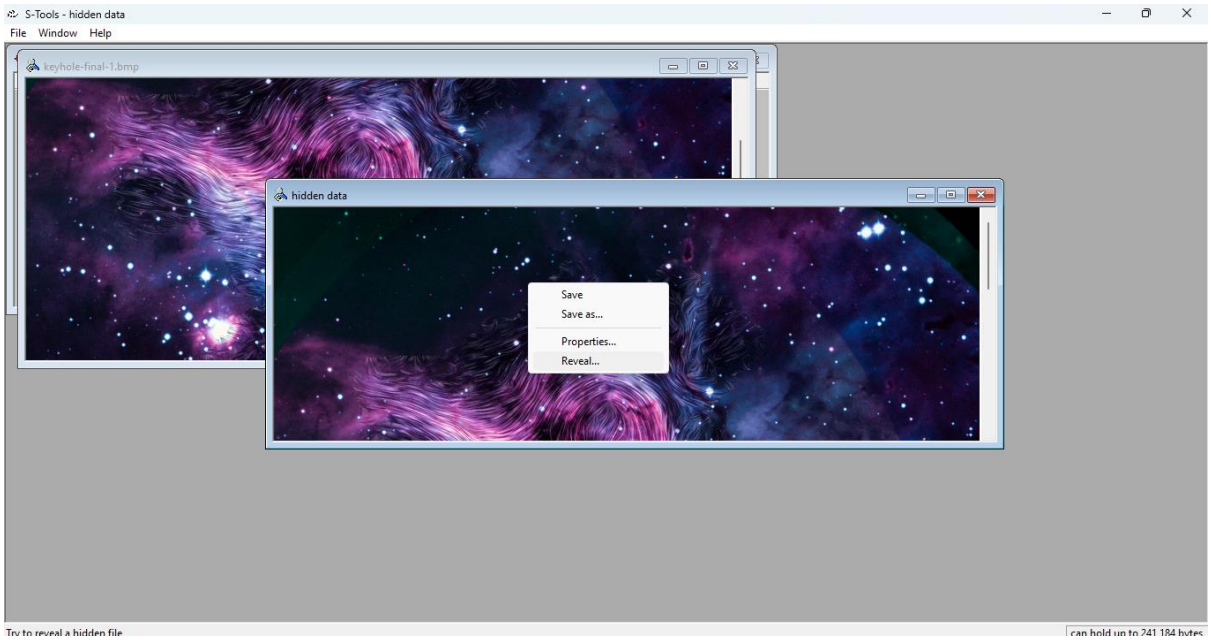


Step 8: Selecting the 'Properties' button while the cursor is over any image will display the following

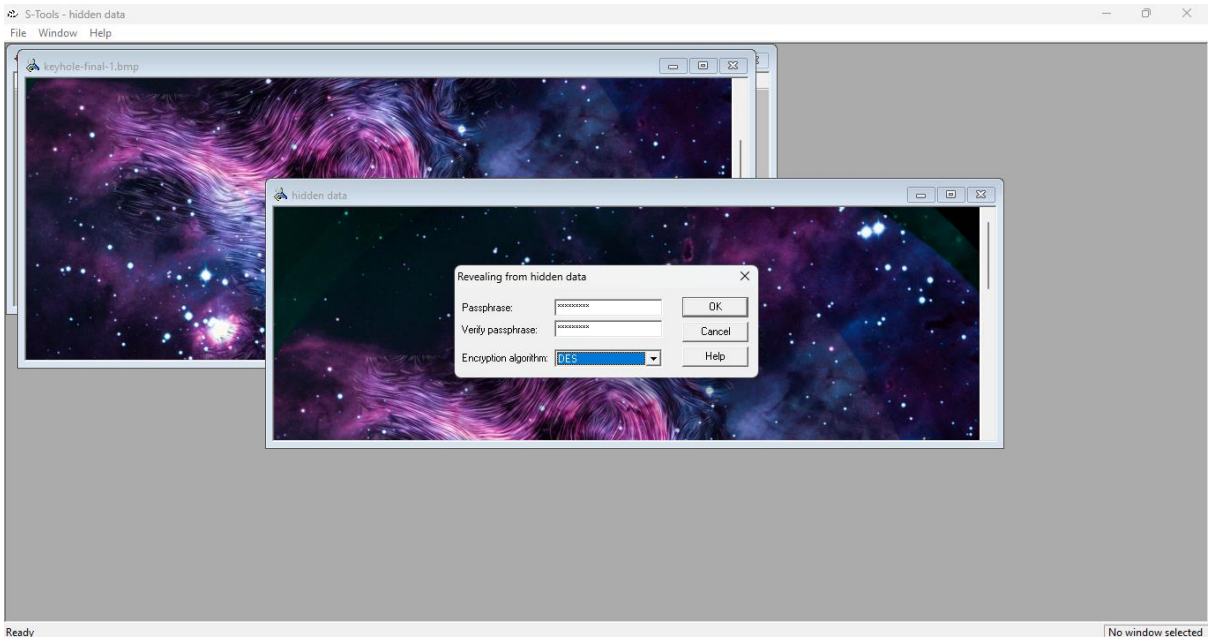
- Width and Height of the image
- Bits per pixel
- Memory Usage (file size in bytes)
- Compression



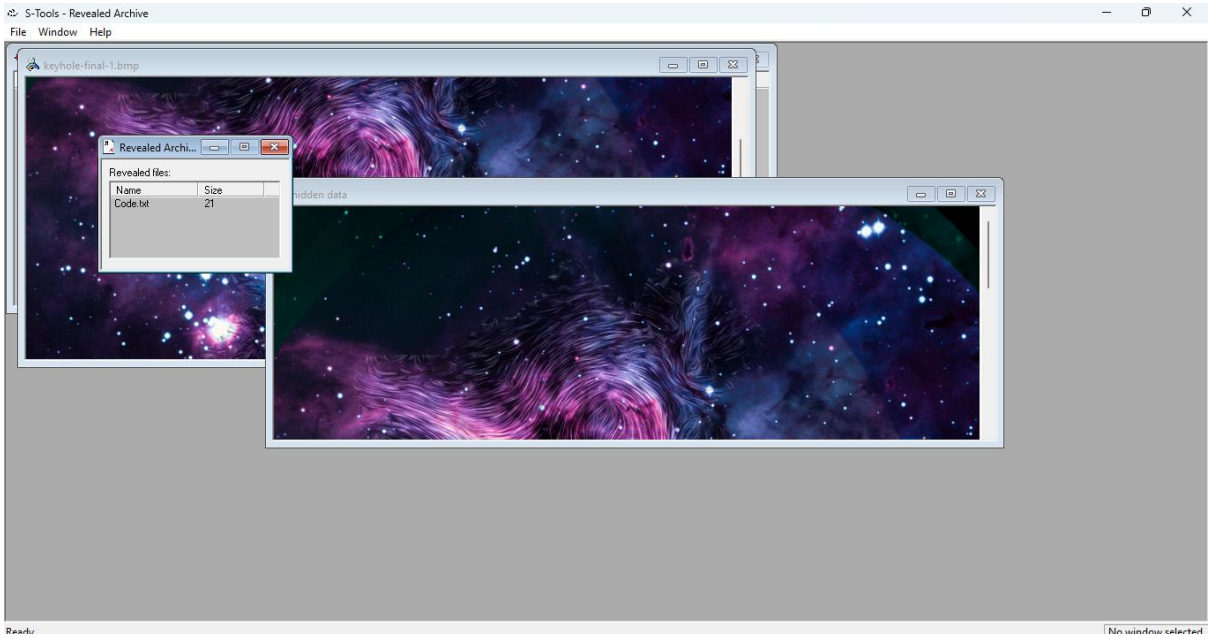
Step 9: Selecting the **'Reveal' button** will display a passphrase dialogue box. A passphrase must be entered twice in the dialogue box and the correct encryption algorithm must be selected.



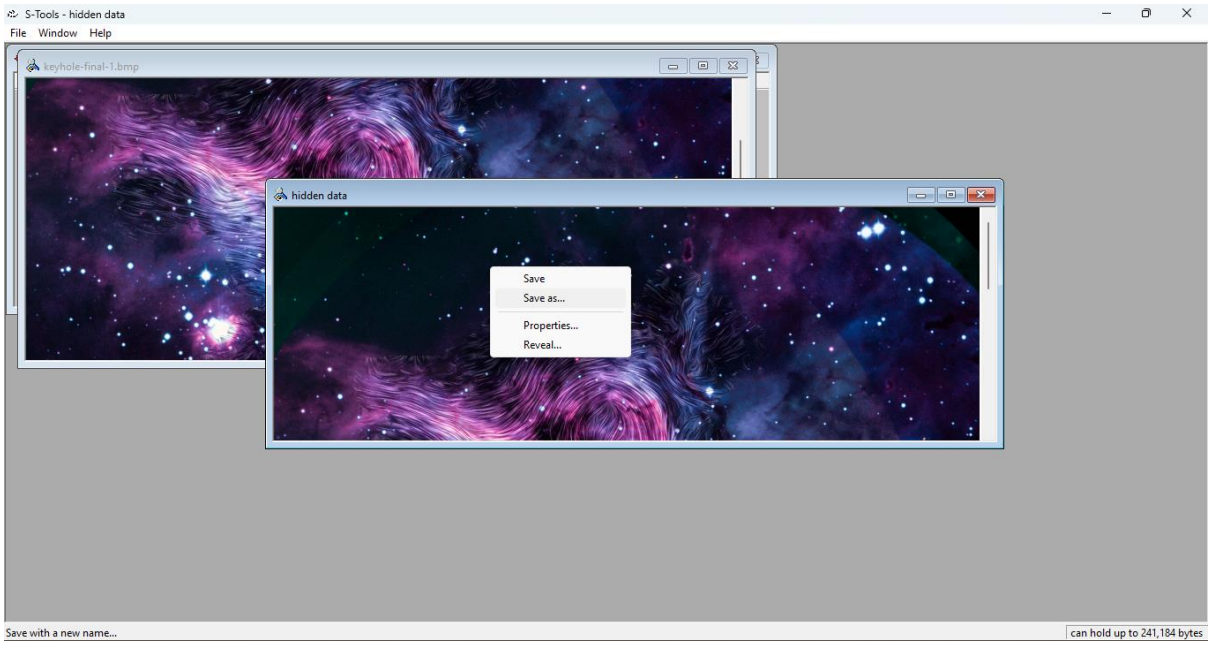
- Enter a passphrase twice, select the encryption algorithm, and **select the 'OK'** button.



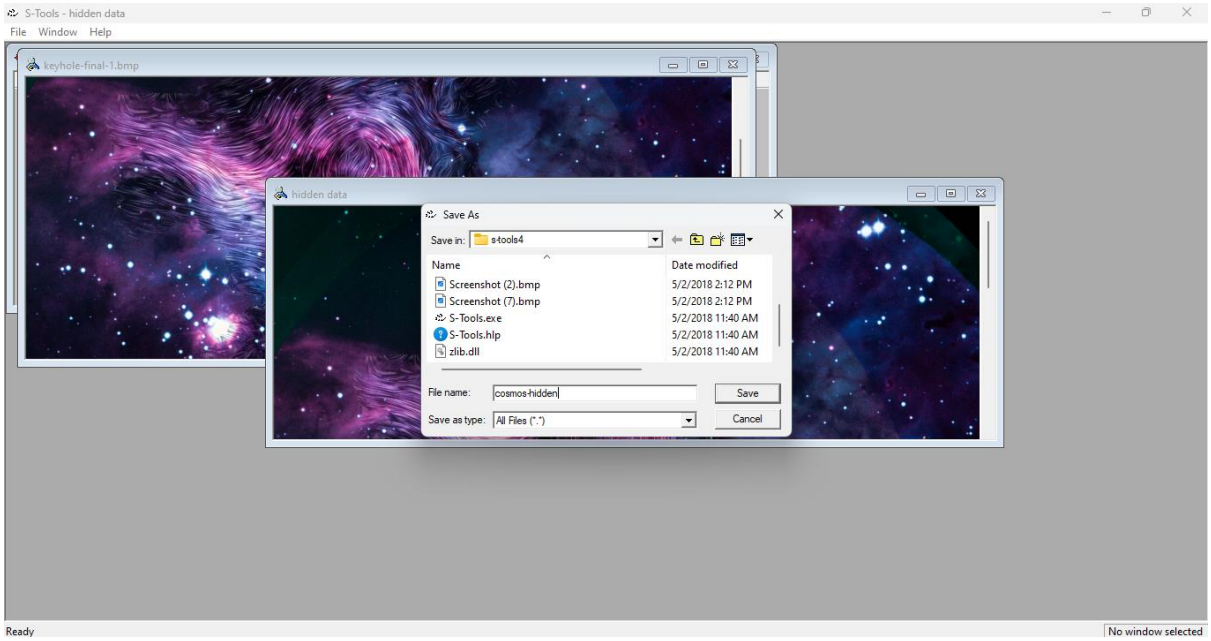
- A ‘Revealed Archive’ dialogue box will display which contains the file name and size of the hidden file.



Step 10: Select the Save as

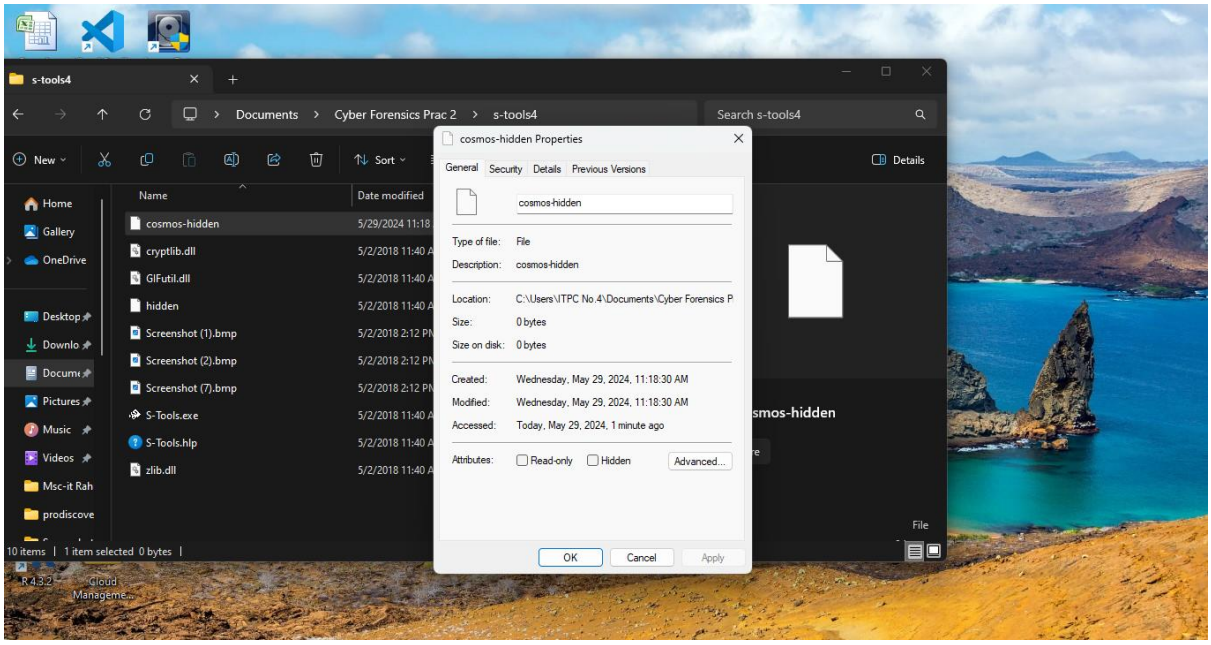


- A ‘Save As’ dialogue box will appear. Enter a valid file name, select the working directory and select the ‘Save’ button



Step 11: Locate the files in the working directory.

- Open the files using a multimedia software program and ensure that the files were extracted from the steganography file successfully.

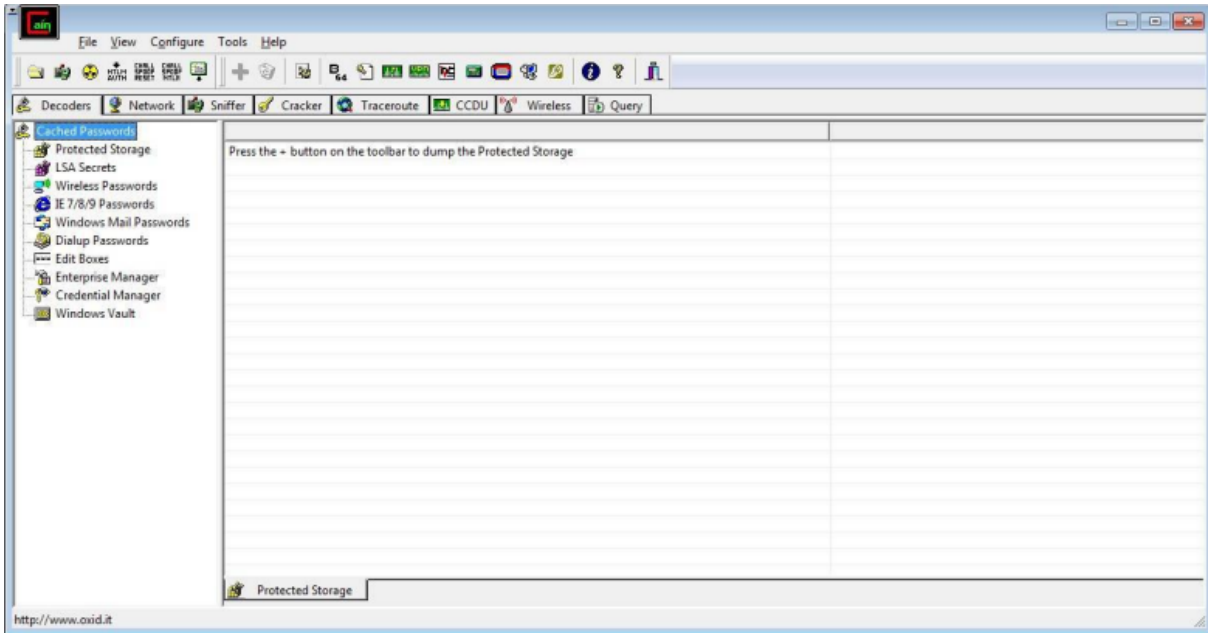


Practical: 7

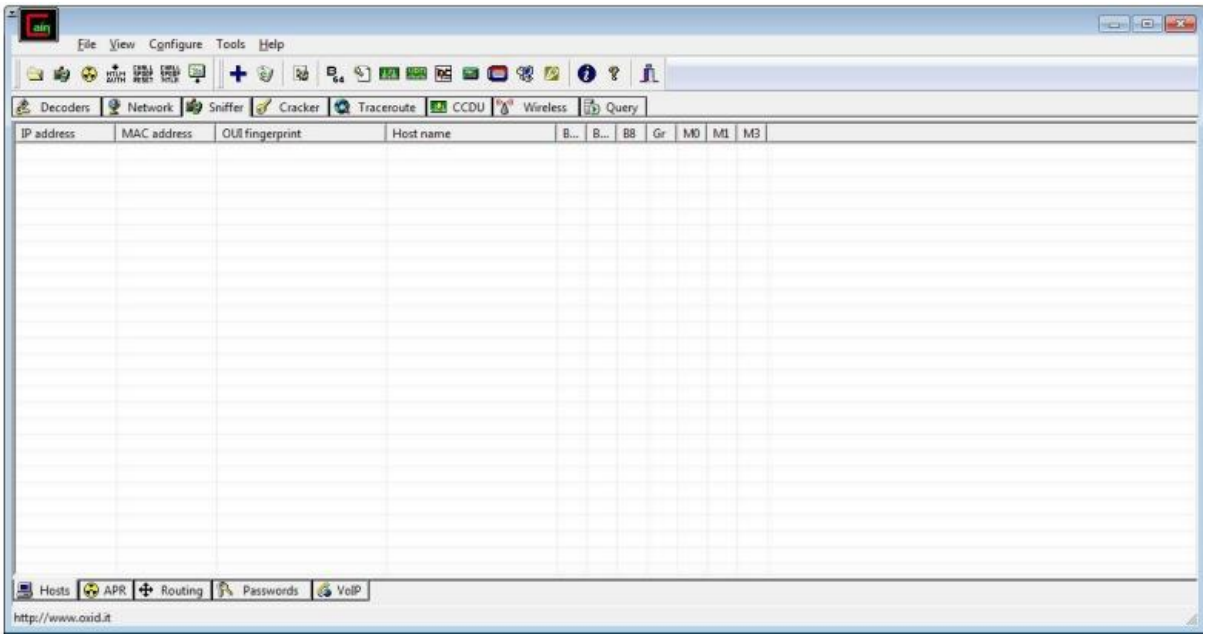
Aim: Performing Sniffing and Password Cracking Using Cain and Abel.

Writeup:

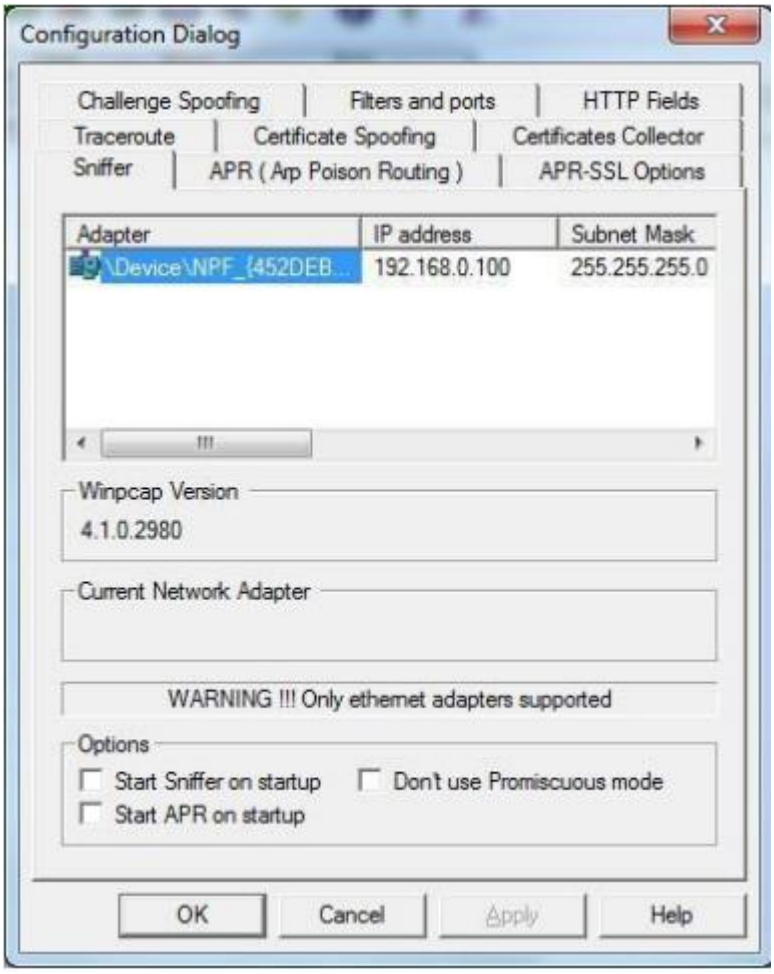
Step 1: Install and open cain and abel.



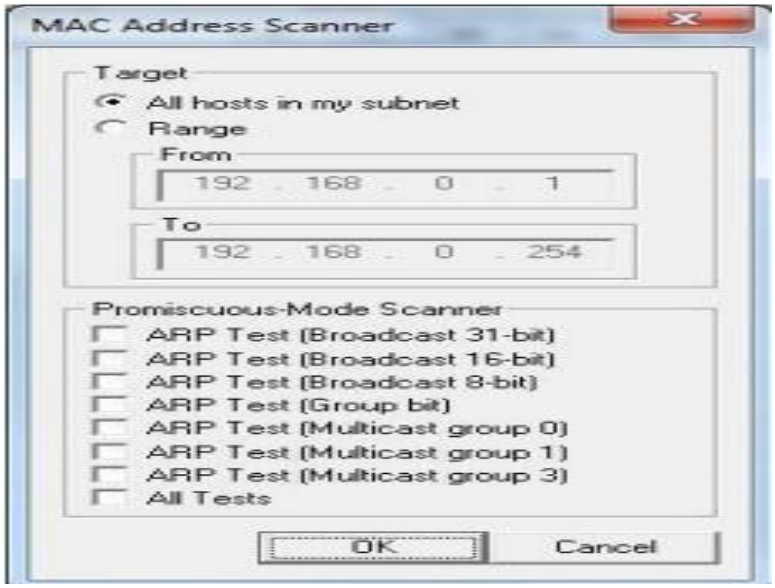
Step 2: Select sniffer on the top.



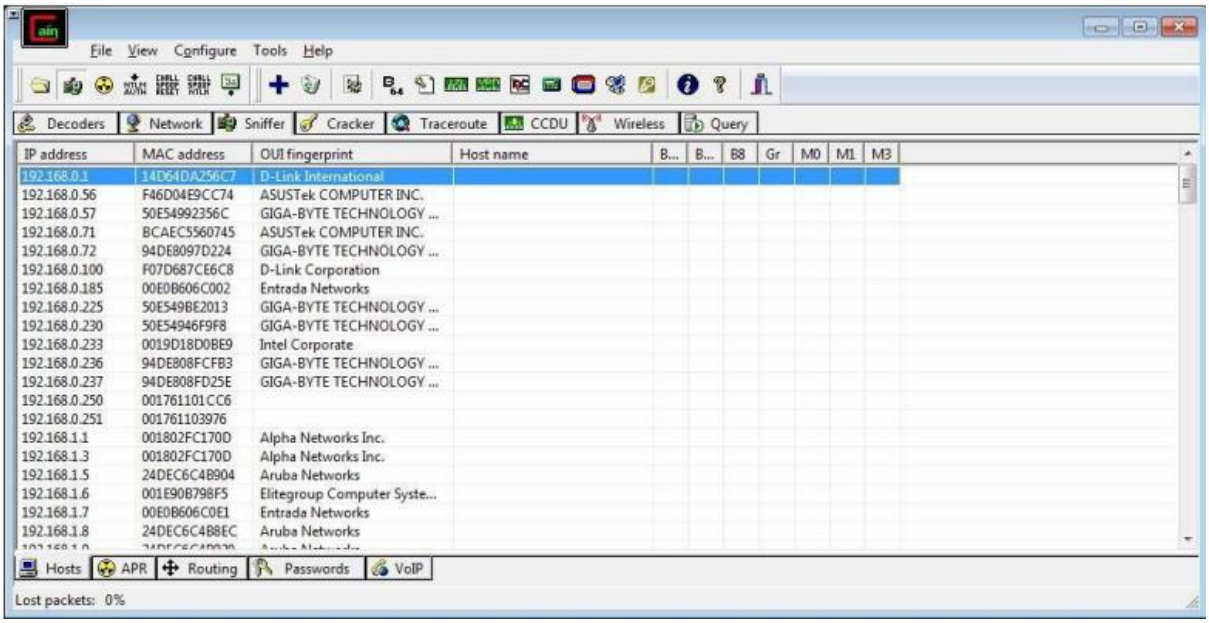
Step 3: Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



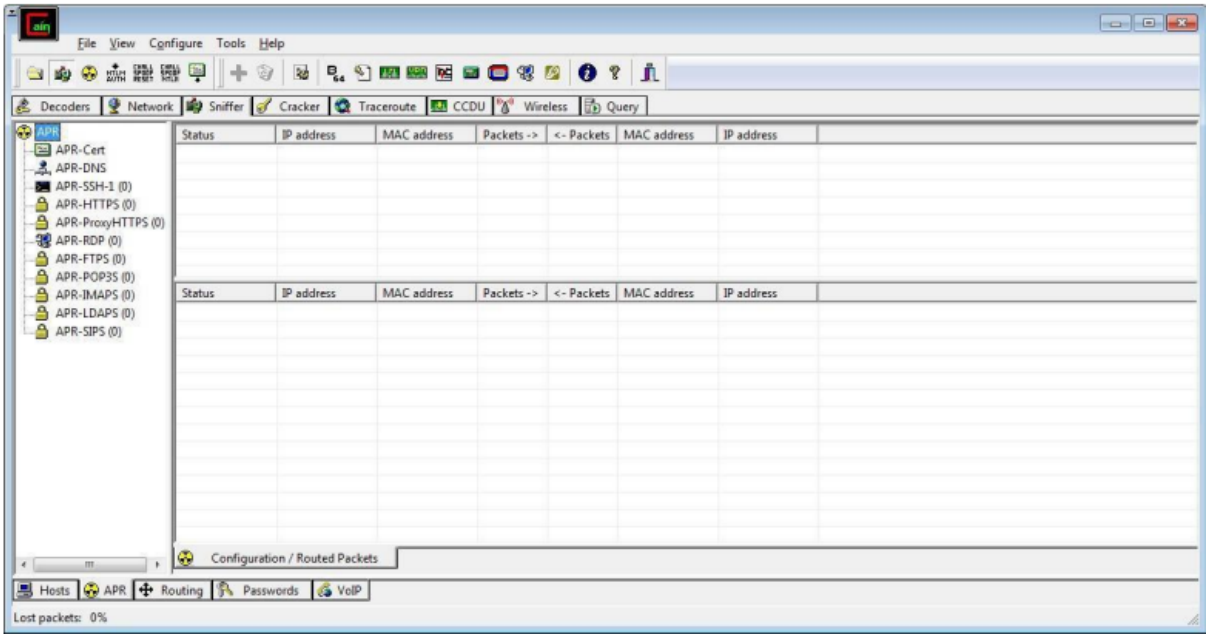
Step 4: Click on "+" icon on the top. Click on ok.



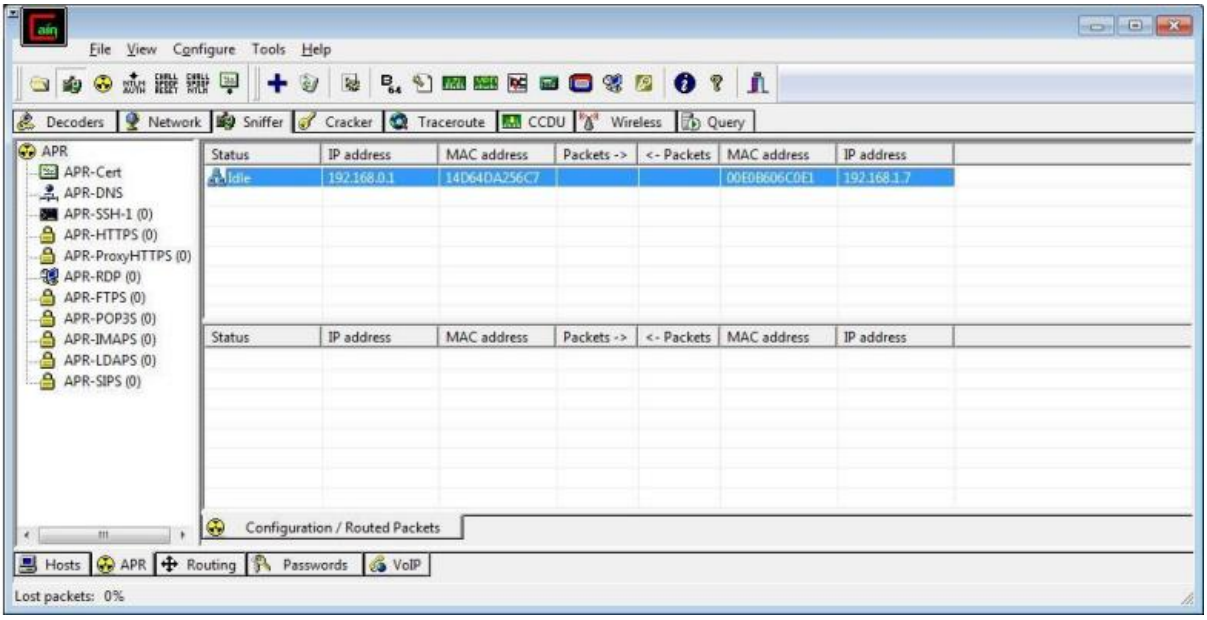
Step 5: Shows the Connected host.



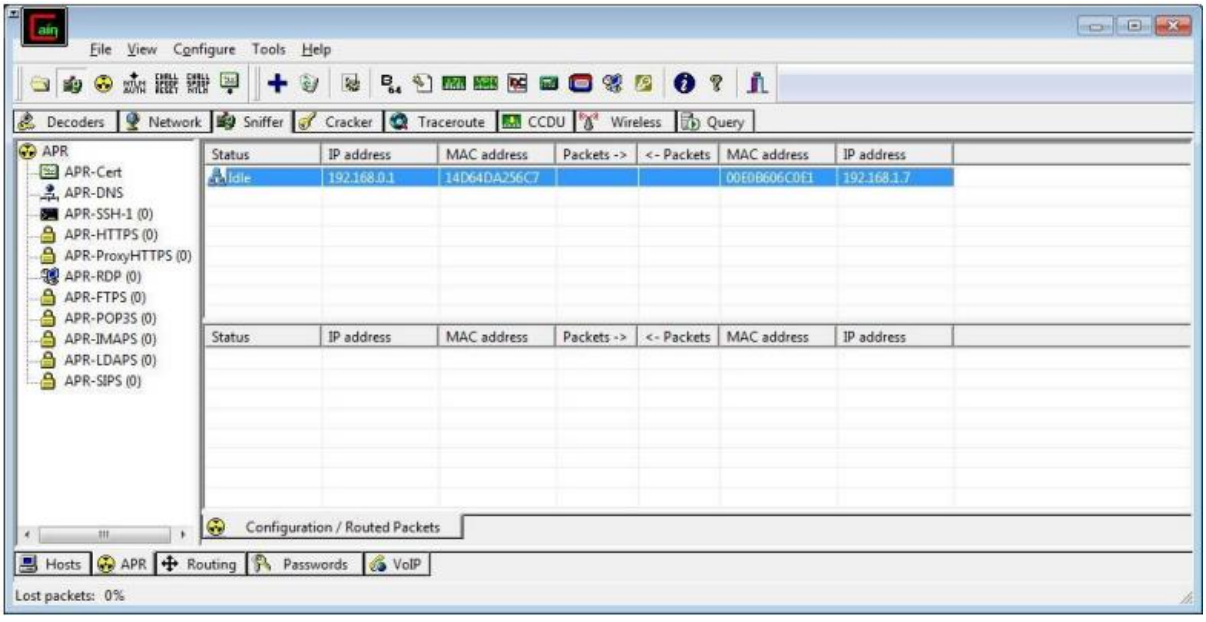
Step 6: Select Arp at bottom.



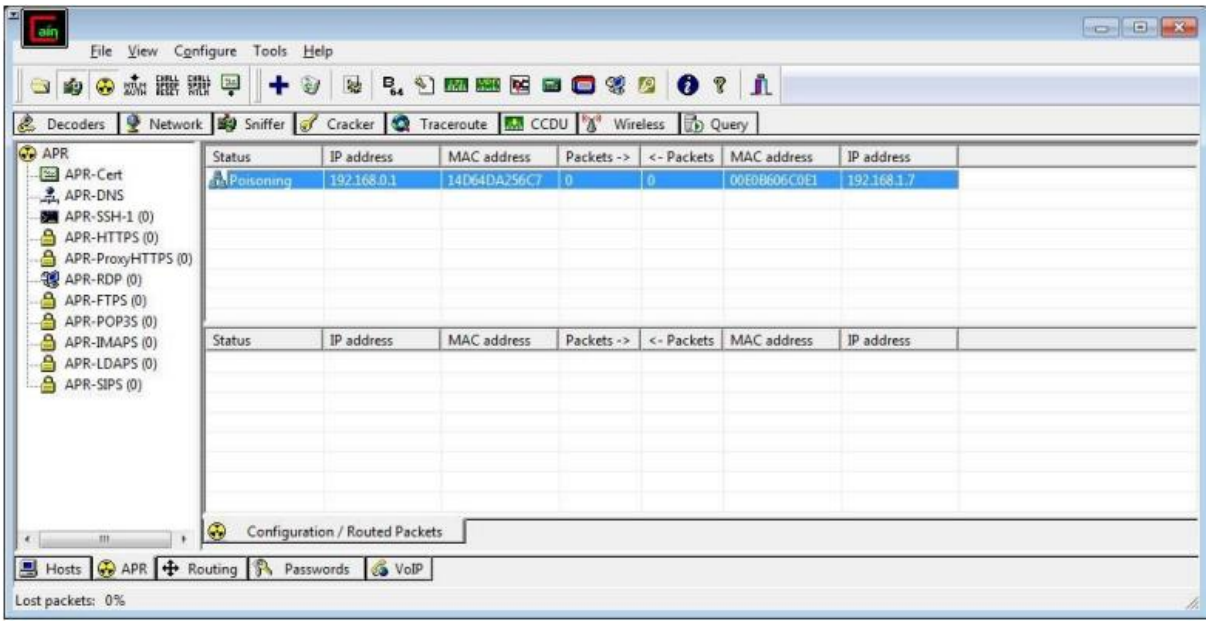
Step 7: Click on "+" icon at the top.



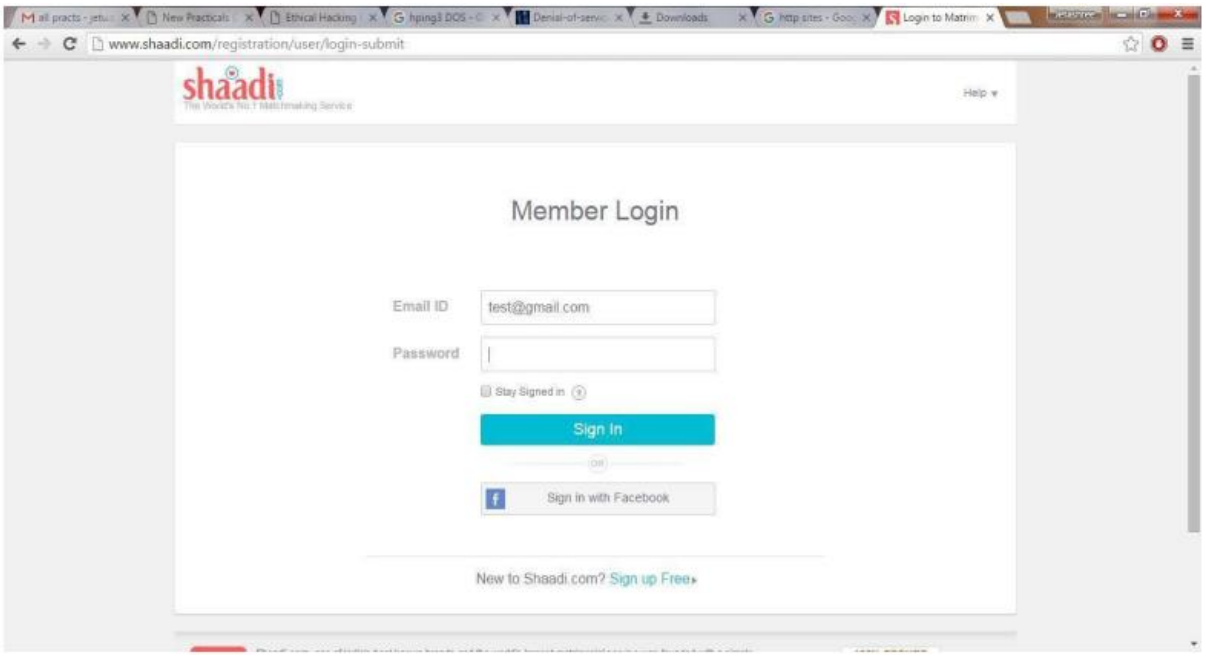
Step 8: Click on start/stop ARP icon on top.



Step 9: Poisoning the source.



Step 10: Go to any website on source ip address.



Step 11: Go to password option in the cain & abel and see the visited site password